

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
SHERMAN DIVISION

BRIAN HUDDLESTON,

Plaintiff,

v.

FEDERAL BUREAU OF  
INVESTIGATION and UNITED  
STATES DEPARTMENT OF JUSTICE,

Defendants.

CIVIL ACTION No. 4:20CV00447

**EXHIBIT A**



U.S. Department of Justice

**Federal Bureau of Investigation**  
Washington, D.C. 20535

December 9, 2022

MR. BRIAN HUDDLESTON  
C/O MR. TY O. CLEVENGER  
212 S. OXFORD STREET #7D  
BROOKLYN, NY 11217

FOIPA Request No.: 1465531-000  
Subject: Seth Rich (January 1, 2016 to present)

*Brian Huddleston v. Federal Bureau of  
Investigation, et al*  
Civil Action No.: 4:20-cv-00447

Dear Mr. Huddleston:

The FBI has completed its review of records subject to the Freedom of Information/Privacy Acts (FOIPA) that are responsive to your request. The enclosed documents were reviewed under the FOIA, Title 5, United States Code, Section 552. Below you will find checked boxes under applicable statutes for the exemptions asserted to protect information exempt from disclosure. The appropriate exemptions are noted on the processed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely pursuant to applicable exemptions. An Explanation of Exemptions is enclosed to further explain justification for withheld information.

**Section 552**☐ (b)(1)☐ (b)(2)☒ (b)(3)50 USC § 3024(i)(1)☐ (b)(4)☐ (b)(5)☒ (b)(6)☒ (b)(7)(A)☐ (b)(7)(B)☒ (b)(7)(C)☐ (b)(7)(D)☒ (b)(7)(E)☐ (b)(7)(F)☐ (b)(8)☐ (b)(9)**Section 552a**☐ (d)(5)☐ (j)(2)☐ (k)(1)☐ (k)(2)☐ (k)(3)☐ (k)(4)☐ (k)(5)☐ (k)(6)☐ (k)(7)

7 pages were reviewed and 0 pages are being released.

Please see the paragraphs below for relevant information specific to your request and the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

☐ Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].

☐ This information has been referred to the OGA(s) for review and direct response to you.

☐ We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. "Part 1" of the Addendum includes standard responses that apply to all requests. "Part 2" includes additional standard responses that apply to all requests for records about yourself or any third party individuals. "Part 3" includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

Although your request is in litigation, we are required by law to provide you the following information:

If you are not satisfied with the Federal Bureau of Investigation's determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by emailing the FBI's FOIA Public Liaison at [foipaquestions@fbi.gov](mailto:foipaquestions@fbi.gov). The subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified. You may also contact the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at [ogis@nara.gov](mailto:ogis@nara.gov); telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Please direct any further inquiries about this case to the Attorney representing the Government in this matter. Please use the FOIPA Request Number and/or Civil Action Number in all correspondence or inquiries concerning your request.



See additional information which follows.

Sincerely,



Michael G. Seidel  
Section Chief  
Record/Information  
Dissemination Section  
Information Management Division

#### Enclosures

In response to your Freedom of Information Act (FOIA) request and subsequent civil action case pending in the U.S. District Court for the Eastern District of Texas, enclosed is a Deleted Page Information Sheet (DPIS) representing pages Bates Stamped FBI (20-cv-00447)-1802 through FBI (20-cv-00447)-1808 which have been withheld in their entirety pursuant to applicable FOIA Exemptions.

These pages were located in cross-reference files as described below. No "main" investigative files pertaining to the subject of your request were located.

Cross-references are defined as mentions of the subject of your request in files to other individuals, organizations, events, or activities. In processing the cross-references, the pages considered for possible release included only those pages which mention the subject of your request and any additional pages showing the context in which the subject of your request was mentioned. The cross-references were processed pursuant to the provisions of the FOIA and are being released to you in redacted form.

## FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.

## Part 1: The standard responses below apply to all requests:

- (i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on [the www.fbi.gov/foia website](https://www.fbi.gov/foia).
- (ii) **Intelligence Records.** To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that any such records do or do not exist.

## Part 2: The standard responses below apply to all requests for records on individuals:

- (i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.
- (ii) **Requests for Records about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.
- (iii) **Requests for Confidential Informant Records.** The FBI can neither confirm nor deny the existence of confidential informant records pursuant to FOIA exemptions (b)(7)(D), (b)(7)(E), and (b)(7)(F) [5 U.S.C. §§ 552 (b)(7)(D), (b)(7)(E), and (b)(7)(F)] and Privacy Act exemption (j)(2) [5 U.S.C. § 552a (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records would reveal confidential informant identities and information, expose law enforcement techniques, and endanger the life or physical safety of individuals. This is a standard response and should not be read to indicate that such records do or do not exist.

## Part 3: General Information:

- (i) **Record Searches and Standard Search Policy.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems, such as the Central Records System (CRS), or locations where responsive records would reasonably be found. The CRS is an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. The standard search policy is a search for main entity records in the CRS. Unless specifically requested, a standard search does not include a search for reference entity records, administrative records of previous FOIPA requests, or civil litigation files.
  - a. *Main Entity Records* – created for individuals or non-individuals who are the subjects or the focus of an investigation
  - b. *Reference Entity Records* – created for individuals or non-individuals who are associated with a case but are not known subjects or the focus of an investigation
- (ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.
- (iii) **Foreseeable Harm Standard.** As amended in 2016, the Freedom of Information Act provides that a federal agency may withhold responsive records only if: (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the nine exemptions that FOIA enumerates, or (2) disclosure is prohibited by law (5 United States Code, Section 552(a)(8)(A)(i)). The FBI considers this foreseeable harm standard in the processing of its requests.
- (iv) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheet. These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at [www.fbi.gov/about-us/cjis/identity-history-summary-checks](https://www.fbi.gov/about-us/cjis/identity-history-summary-checks). Additionally, requests can be submitted electronically at [www.edo.cjis.gov](https://www.edo.cjis.gov). For additional information, please contact CJIS directly at (304) 625-5590.

**EXPLANATION OF EXEMPTIONS****SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information ( A ) could reasonably be expected to interfere with enforcement proceedings, ( B ) would deprive a person of a right to a fair trial or an impartial adjudication, ( C ) could reasonably be expected to constitute an unwarranted invasion of personal privacy, ( D ) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, ( E ) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or ( F ) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

**SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a**

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

**FEDERAL BUREAU OF INVESTIGATION****FOI/PA****DELETED PAGE INFORMATION SHEET****Civil Action# 4:20-cv-00447****Total Withheld Page(s) = 7**

<b>Bates Page Reference FBI (20-cv-00447)-</b>	<b>Reason for Withholding</b> (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)
1802	b7A-1; b3-1; b6-1; b7C-1; b7E-2, 3, 9; (1 page)
1803	b7A-1; b3-1; b6-1; b7C-1; b7E-2, 3, 9; (1 page)
1804	b7A-1; b3-1; b6-1; b7C-1; b7E-2, 3, 6, 10; (1 page)
1805	b7A-1; b3-1; b6-1, 4, 5; b7C-1, 4, 5; b7E-2, 3, 6, 10; (1 page)
1806	b7A-1; b3-1; b6-1, 4; b7C-1, 4; b7E-2, 6; (1 page)
1807	b7A-1; b6-1; b7C-1; (1 page)
1808	b7A-1; b6-1, 4; b7C-1, 4; (1 page)

XXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXX

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
SHERMAN DIVISION

BRIAN HUDDLESTON,

Plaintiff,

v.

FEDERAL BUREAU OF  
INVESTIGATION and UNITED  
STATES DEPARTMENT OF JUSTICE,

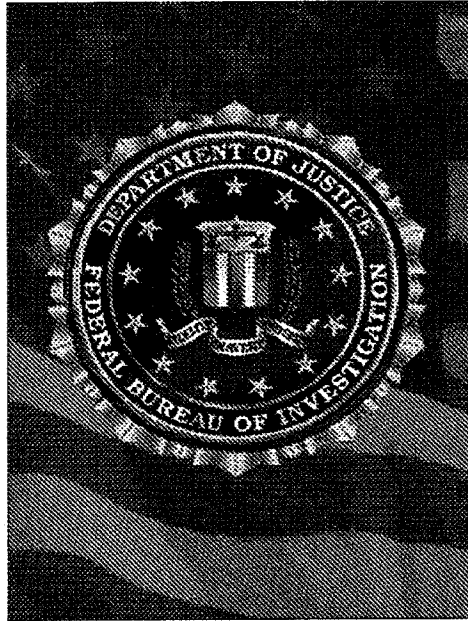
Defendants.

CIVIL ACTION No. 4:20CV00447

**EXHIBIT B**

UNCLASSIFIED//~~LES~~  
(U) Digital Evidence Policy Guide

## **(U) Digital Evidence Policy Guide**



**(U) Federal Bureau of Investigation**

**(U) Operational Technology Division**

**(U) 0830PG**

**(U) July 31, 2016**

UNCLASSIFIED//~~LES~~

**UNCLASSIFIED//~~LES~~**  
(U) Digital Evidence Policy Guide

**(U) General Information**

(U) Questions or comments pertaining to this policy guide can be directed to:

(U) Federal Bureau of Investigation Headquarters, Operational Technology Division

(U) Division point of contact: division policy officer,

b6 -1  
b7C -1  
b7E -1

**(U) Supersession Information**

(U) This policy guide supersedes the *Digital Evidence Policy Directive and Policy Guide*, 0639DPG.

(U) This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit listed in the contact section of this policy guide.

(U) This policy guide is solely for the purpose of internal FBI guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor does it place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice (DOJ) and the FBI.

**(U) DIOG Provision**

(U) No policy or PG may contradict, alter or otherwise modify the standards of the *Domestic Investigations and Operations Policy Guide* (DIOG). Requests for DIOG modifications can be made to the Internal Policy office (IPO) pursuant to DIOG subsection 3.2.2, paragraphs (A), (B), (C), and (D).

**(U) Law Enforcement Sensitive ~~LES~~**

The information marked (U//~~LES~~) in this document is the property of the Federal Bureau of Investigation and is for internal use within the FBI only. Distribution outside the FBI without Operational Technology Division authorization is prohibited. Precautions must be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a Web site on an unclassified network.

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

## (U) Table of Contents

1. (U) Introduction .....	1
1.1. (U) Purpose .....	1
1.2. (U) Background .....	1
1.3. (U) Scope .....	2
1.4. (U) [REDACTED] of Digital Evidence .....	b3 -1 b7E -2, 3, 4, 5
1.4.1. (U) Digital Evidence Searches Under [REDACTED] .....	2
1.4.2. (U) Reviews or Examinations of Digital Evidence in [REDACTED] .....	3
1.5. (U) Intended Audience .....	4
2. (U) Roles and Responsibilities .....	5
2.1. (U) Digital Evidence Roles .....	8
2.2. (U) Digital Evidence Responsibilities .....	8
2.2.1. (U) FBI Personnel Who Handle, Process, or Perform Content Reviews of Digital Evidence .....	8
2.2.2. (U) Federal Bureau of Investigation Headquarters .....	10
2.2.3. (U) FBI Field Offices .....	12
3. (U) Policies .....	14
4. (U) Procedures and Processes .....	15
4.1. (U// <del>FOUO</del> ) Forensic Program Compliance Within the FBI .....	15
4.2. (U) Digital Evidence Handling .....	15
4.2.1. (U) Personnel Authorized to Handle Digital Evidence .....	15
4.2.2. (U) Presearch Considerations .....	15b7E -3, 4, 5
4.2.3. (U) Timeframe for Warrants Involving Digital Evidence .....	15
4.2.4. (U) Consent Searches for Digital Evidence .....	15
4.3. (U) Digital Evidence Processing .....	20
4.3.1. (U) Imaging .....	20
4.3.2. (U) [REDACTED] .....	20
4.3.3. (U) [REDACTED] .....	20
4.3.4. (U) Performing Content Reviews .....	21

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

4.3.5. (U) Documenting Review of DE .....	23
4.3.6. (U) Copies .....	28
4.3.7. (U) Approved Tools .....	34
4.3.8. (U) [REDACTED] .....	35 <sup>b7E -3, 4, 5</sup>
4.3.9. (U) [REDACTED] .....	35
4.3.10. (U) Reexaminations .....	37
4.3.11. (U) Advanced Technical Analysis .....	39
4.3.12. (U) Assigning Requests to Examiners and Digital Evidence Backlog Definition .....	40
4.4. (U) Testifying Regarding Digital Evidence Processing .....	40
4.4.1. (U) Computer Analysis and Response Team Forensic Examiners; Forensic Audio, Video and Image Analysis Unit Examiners; Computer Scientists-Field Office; and Operational Technology Division, Digital Forensics and Analysis Section Technical Experts .....	40
4.4.2. (U) Digital Extraction Technicians and Computer Analysis and Response Team Technicians .....	41
4.5. (U) Seeking Legal Advice .....	41
5. (U) Summary of Legal Authorities .....	42
6. (U) Recordkeeping Requirements .....	43
6.1. (U// <del>LES</del> ) FBI Central Recordkeeping System .....	43
6.2. (U) Additional Information on Recordkeeping and Forms Use .....	43

**(U) List of Appendices**

Appendix A: (U) Final Approvals .....	A-1
Appendix B: (U) Sources of Additional Information .....	B-1
Appendix C: (U) Contact Information .....	C-1
Appendix D: (U) Definitions and Acronyms .....	D-1
Appendix E: (U// <del>LES</del> ) Examination of FBI Evidence [REDACTED] .....	E-1
[REDACTED] .....	E-1

b7E -3, 4, 5

UNCLASSIFIED//~~LES~~  
(U) Digital Evidence Policy Guide

**(U) Table of Figures**

Figure 1. (U// <del>FOUO</del> ) [REDACTED] .....	b7E -3, 4 , 5
Figure 2. (U// <del>FOUO</del> ) Digital Evidence Copies .....	28
Figure 3. (U// <del>FOUO</del> ) [REDACTED] .....	D-1

**(U) List of Tables**

Table 1. (U) Roles and Responsibilities .....	8
---	---

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

## 1. (U) Introduction

### 1.1. (U) Purpose

(U//~~FOUO~~) This policy guide (PG) establishes and consolidates the policies and procedures for the proper handling, reviewing, and processing of digital evidence (DE) for the Federal Bureau of Investigation (FBI), whether it is seized, received, or otherwise legally obtained. Digital evidence is data that is stored or transmitted in binary form and is obtained with the intent to assist in proving or disproving a matter at issue in a case or an investigation. Digital evidence includes binary data stored on magnetic, optical, or mechanical storage devices, including, but not limited to, integrated circuits, microcontrollers, chips, tapes, computers, cell phones, compact discs (CD)/digital video discs (DVD), flash drives, random-access memory (RAM), magneto optical cartridges, Universal Serial Bus (USB) microstorage devices (commonly known as "thumb drives"), digital video recorders (DVR), or other electronic devices that store or process data digitally. The Operational Technology Division (OTD) Digital Forensics and Analysis Section (DFAS) is responsible for the FBI's DE program and for establishing DE policies.

(U//~~FOUO~~) Except as noted below, this PG applies to all DE obtained or acquired by the FBI in connection with an investigation.

(U//~~FOUO~~) This PG does not apply to digital evidence obtained through:

- (U//~~FOUO~~) [REDACTED] b7E -3, 4, 5
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) Information originally obtained in a nondigital format that was later converted to digital form to facilitate storage, retrieval, or search/query.
- (U//~~FOUO~~) Specialized evidentiary information or data collections regulated by another PG (e.g., digital fingerprints, digital DNA (deoxyribonucleic acid) profile databases).
- (U//~~FOUO~~) Business, transactional, or other records obtained through a subpoena [REDACTED] b7E -3, 4, 5  
[REDACTED] and were provided in digital form.

(U//~~FOUO~~) However, if exempted records are later submitted for a forensic examination, this PG would apply to the examination of those materials.

### 1.2. (U) Background

(U//~~FOUO~~) As computer technology has advanced over time, digital devices have become universally used to include individuals, groups, or organizations violating federal laws [REDACTED] b7E -3, 4, 5  
[REDACTED] DE is ever-present in FBI investigations and operations. All personnel who encounter DE must understand how to properly handle, review, and process it to avoid damaging the integrity of the evidence or violating the constitutional rights of a person during the course of an investigation.

(U//~~FOUO~~) The FBI requires that DE be seized, searched, stored, copied, processed, reviewed, examined, analyzed, presented, and disposed of in a scientifically proven and legally defensible manner to maximize its integrity, authenticity, probative value, and evidentiary reliability, and to facilitate the DE's admissibility at trial or other adjudicative proceeding. DE is malleable and can

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

be easily altered or destroyed (e.g., by viewing or copying files without following the proper procedures or by variance in temperature or exposure to heat or magnetic fields). Utilizing properly trained personnel, established procedures, approved tools, and an appropriate quality assurance (QA) program maximizes the reliability and integrity of DE for the purposes of authentication and presentation in court, as well as for investigative [REDACTED]

b7E -3, 4, 5

### 1.3. (U) Scope

(U//~~FOUO~~//LES) This PG addresses handling, processing, and performing content reviews of DE. Handling includes procedures related to on-scene search and seizure, transportation and storage, evidence intake, and shipping. Processing of DE includes detailed procedures related to on-scene preview, imaging, memory capture, performing a content review, search, extraction, report preparation, and advanced technical analysis [REDACTED]

b7E -3, 4, 5

[REDACTED]  
[REDACTED] Performing a content review involves the viewing of the [REDACTED]  
[REDACTED] DE container(s) in accordance with the scope of legal authority.

### 1.4. (U) [REDACTED]

(U//~~FOUO~~) Unless expressly stated otherwise, this PG applies equally to criminal [REDACTED]  
[REDACTED] FBI personnel should coordinate questions concerning legal authority required for [REDACTED] of DE with their chief division counsels (CDC) or associate division counsels (ADC) or with the Office of the General Counsel (OGC), [REDACTED]  
[REDACTED]

#### 1.4.1. (U) [REDACTED]

(U//~~FOUO~~) [REDACTED]

b3 -1

b7E -2, 3, 4, 5, 6

(U//~~FOUO~~) [REDACTED]  
[REDACTED]  
[REDACTED]  
(U//~~FOUO~~) [REDACTED]  
[REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

1.4.2. (U) Reviews or Examinations of Digital Evidence in [REDACTED]

(U//~~FOUO~~) The following subsections discuss some of the unique areas of concern raised when the FBI or [REDACTED]

1.4.2.1. (U)

(U//~~FOUO~~) [REDACTED]

(U//~~FOUO~~) However, investigative personnel may review or analyze evidence seized under the authority of a criminal warrant or consent when the evidence at issue has been determined to be within the scope of the criminal warrant or consent pursuant to which it was seized. FBI personnel must not expand the search beyond the consent or criminal warrant's scope. FBI personnel should coordinate questions concerning their authority under this scenario with their servicing CDCs/ADCs and OGC [REDACTED]

(U//~~FOUO~~) In the event that the FBI [REDACTED] need to conduct a search of criminally seized DE beyond the scope of the criminal warrant or consent, they should coordinate with their CDCs/ADCs, OGC [REDACTED] and must notify the AUSA to obtain additional legal authority [REDACTED]

1.4.2.1.1. (U) Use of Analytical Tools or Database Systems to Review or Examine Digital Evidence

(U//~~FOUO~~) In [REDACTED] FBI personnel may [REDACTED]

evidence must be tagged in some manner to permit its withdrawal from the holdings [REDACTED]

(U//~~FOUO~~) Before uploading DE seized [REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

1.4.2.2.

(U)

(U//~~FOUO~~) Often during reviews or examinations of DE [REDACTED]

[REDACTED] (when providing technical assistance to the FBI [REDACTED] b3 -1  
[REDACTED] may be employed in accordance with the provisions b7E -2, 3, 4, 5  
of this PG. DOJ policy requires the approval of the deputy Attorney General (DAG) [REDACTED]  
[REDACTED] in the furtherance of a criminal case. See  
[REDACTED]  
[REDACTED] for more information.

1.4.2.2.1.

(U//~~LES~~)

(U//~~LES~~) During the course of [REDACTED]

[REDACTED]

(U//~~LES~~)

[REDACTED]

b3 -1  
b7E -2, 3, 4, 5, 6

(U//~~FOUO~~) When this circumstance applies, the case agent is responsible for notifying and coordinating with his or her CDC/ADC and OGC [REDACTED] To ensure that appropriate disclosures are made, case agents must coordinate with the appropriate assistant United States attorney (AUSA) or DOJ trial attorney.

### 1.5. (U) Intended Audience

(U//~~FOUO~~) This PG applies to all personnel working for or with the FBI, including FBI employees, contractors, detailees, and task force personnel assigned to FBI field offices, FBI Headquarters (FBIHQ) divisions, legal attaché (Legat) offices, regional computer forensics laboratories (RCFL), and joint task forces (JTF) that encounter, handle, review, or process DE.

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

## 2. (U) Roles and Responsibilities

### 2.1. (U) Digital Evidence Roles

(U//~~FOUO~~) The FBI's Digital Evidence Program divides DE work functions into general categories or levels based upon the type and complexity of work performed at each level and the training and experience required of FBI personnel to competently perform the duties at each level. Each category of work depicted below in Figure 1 has its own set of training and procedural requirements. The first tiered category requires less training and fewer procedures, while the upper two categories require more training and expertise, as well as more involved procedures.

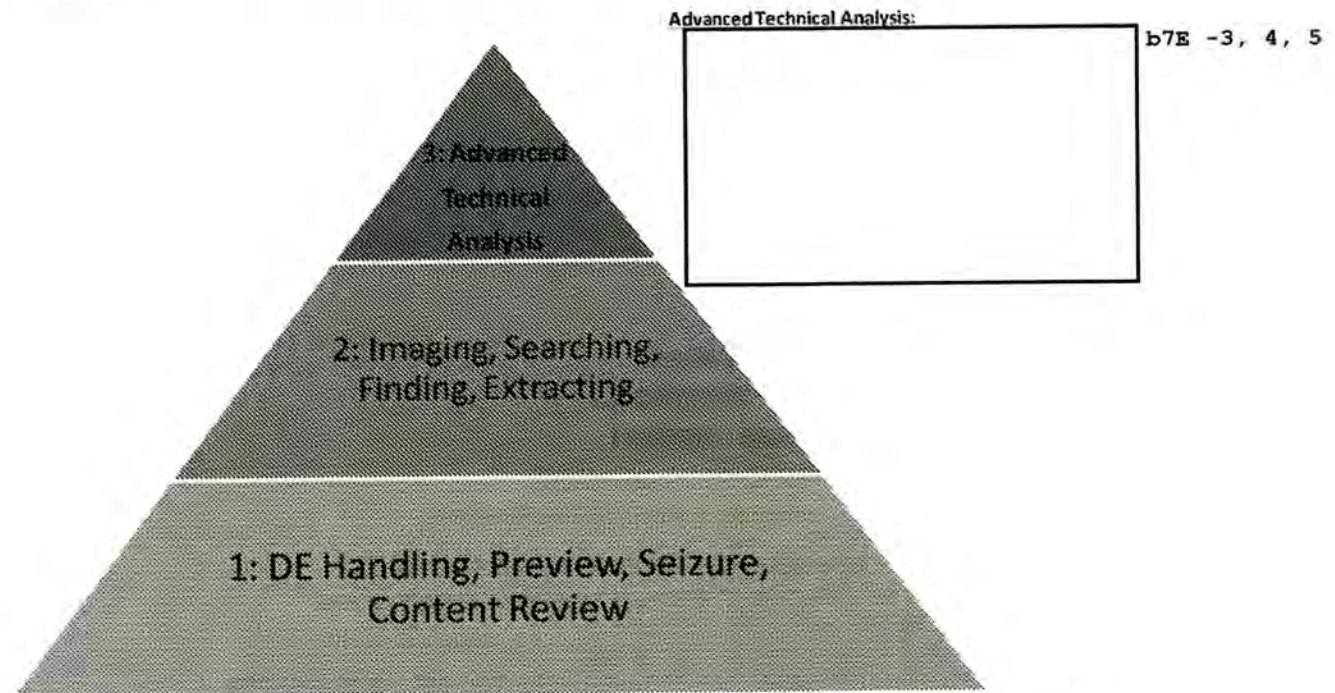


Figure 1. (U//~~FOUO~~) Functional Pyramid

(U//~~FOUO~~) The first tiered category on the pyramid represents the broad population of FBI personnel who, with minimal training, are authorized to handle, preview, seize, and/or review DE content.

(U//~~FOUO~~) The second tiered category represents a smaller population of FBI personnel who have been trained to the technician level, which allows them to image, search, find, and extract DE. The FBI considers the search-and-find function performed by investigative personnel an investigative, as opposed to a forensic, process; however, imaging and extraction remain forensic processes that require training to forensic standards.

(U//~~FOUO~~) The third tiered category represents the smallest population of FBI personnel who have received extensive training and possess the requisite experience necessary to complete the most technically complex DE examinations and analysis.

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

(U//~~FOUO~~) As used throughout this PG, references to training and certification refer to training and certification provided, approved, or recognized by OTD/DFAS. Similarly, unless expressly stated to the contrary, personnel authorized in any tier must comply with the OTD/DFAS-approved training; follow OTD/DFAS-approved policies, procedures, and protocols; and only use tools and/or devices in accordance with this PG and OTD/DFAS policies.

(U//~~FOUO~~) Level 1: The handling of DE for seizure or evidence-control purposes, and/or the preview or review of DE content for investigative [REDACTED] can be performed by b7E -3, 4, 5 personnel such as evidence control technicians (ECT), special agents (SA) and other professional staff personnel who have the proper training and approved tools under procedures approved by OTD/DFAS.

(U//~~FOUO~~) Level 2: DE technician-level work can be performed by the following personnel (who can also perform Level 1 work) under procedures approved by OTD/DFAS:

- (U//~~FOUO~~) Computer Analysis and Response Team (CART) technician (tech): personnel trained and certified to forensically copy or image DE.
- (U//~~FOUO~~) Digital extraction technician (DEXT): personnel trained and certified to copy or image DE and perform simple search/find/extract (SFE) processes on copies of DE.
- (U//~~FOUO~~) Field Audio Video Program (FAVP) forensic analysts (FA): personnel trained and certified to perform basic forensic functions related to audio and video DE.

(U//~~FOUO~~) Level 3: Advanced technical analysis is conducted by the following personnel (who can also perform Level 2 and Level 1 work):

- (U//~~FOUO~~) CART forensic examiner (FE): FBIHQ or field personnel—typically assigned full time to DE work—who are trained, equipped, and certified to copy or image DE, search/find DE, extract data from DE, and provide opinions related to DE, computer forensics, computer or electronic device operations, and other related fields, as their expertise and training permit.
- (U//~~FOUO~~) CART trainees: Prior to achieving CART FE certification, personnel seeking experience and proficiency in the CART program are considered trainees. While in trainee status, these personnel are authorized to perform forensic tasks under the supervision of a certified CART FE:
  - (U//~~FOUO~~) CART on-the-job trainees (OJT): personnel identified by field office management to participate in training with a commitment toward becoming certified CART FEs.
  - (U//~~FOUO~~) CART forensic examiner trainees (FET): personnel assigned to work 100 percent of their time toward CART FE certification. Typically, these are trainees hired into information technology specialist-forensic examiner (ITS-FE) positions. These may also be CART OJTs who are near the end of their training and have committed 100 percent of their time to CART FE work.
- (U//~~FOUO~~) RCFL associate examiner: former certified CART FEs from an agency participating in the RCFL program who have completed their commitment to the RCFL and returned to their home agencies, and who continue a relationship with the RCFL to maintain certification and training. When serving in this role at the RCFL, RCFL

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

associate examiners must continue to be impartial forensic scientists and are prohibited from conducting investigative activities.

- (U//~~FOUO~~) Computer scientist-field operations (CS-FO): CS-FOs are experienced computer scientists who work as integral members of investigative teams supporting FBI investigations and operations. The CS-FO is responsible for providing advanced technical analysis. [REDACTED]

b7E -3, 4, 5

[REDACTED] The CS-FO is not authorized to participate in the collection of data intercept, but may engage in [REDACTED] Additionally, because CS-FOs are part of the investigative team, they are prohibited from performing forensic examinations of DE.

- (U//~~FOUO~~) OTD/DFAS engineer/analyst/forensic examiner: DFAS [REDACTED]

b7E -3, 4, 5

(U) Table 1 depicts the various DE personnel roles and the functions that they are authorized to perform with the proper training and certification.

Functions	Investigative Personnel	CART Tech	DENT	Field CART FEs, CS-FOs, DFAS
<ul style="list-style-type: none"> <li>• DE Handling</li> <li>• Preview</li> <li>• Seizure</li> <li>• Perform Content Reviews</li> </ul>	✓	✓	✓	✓
<ul style="list-style-type: none"> <li>• Imaging</li> </ul>		✓	✓	✓
<ul style="list-style-type: none"> <li>• Search/Find/Extract</li> </ul>			✓	✓

~~UNCLASSIFIED//LES~~ (U)  
(U) Digital Evidence Policy Guide

Functions	Investigative Personnel	CART Tech	DEXT	Field CART FE's, CS-FOs, DFAS
<ul style="list-style-type: none"> <li>Advanced Technical Analysis</li> <li>Role-Specific Standard Operating Procedures (SOPs)</li> </ul>				

**Table 1. (U) Roles and Responsibilities**

**2.2. (U) Digital Evidence Responsibilities**

**2.2.1. (U) FBI Personnel Who Handle, Process, or Perform Content Reviews of Digital Evidence**

(U//~~FOUO~~) All FBI personnel who, because of their positions, handle, process, or perform content reviews of DE, in addition to the specific responsibilities delineated below due to their positions, are responsible for:

- (U//~~FOUO~~) Understanding and complying with the legal authority as it relates to the DE that has been processed, handled, or has had a content review performed.
- (U//~~FOUO~~) Handling, processing, and performing content reviews on DE and documenting those actions in accordance with this PG, other applicable OTD/DFAS policies and procedures, and applicable QA standards.
- (U//~~FOUO~~) Ensuring that all DE is handled, marked, and has a content review performed in accordance with the [REDACTED] b3 -1  
[REDACTED] b7E -2, 3, 4, 5
- (U//~~FOUO~~) Ensuring that all DE is handled, stored, marked, and has a content review performed, in accordance with FBI dissemination marking policies and OTD/DFAS policies.
- (U//~~FOUO~~) Maintaining the chain of custody of all DE.
- (U//~~FOUO~~) Disseminating DE only in accordance with this PG.
- (U//~~FOUO~~) Providing testimony, as required, in any legal proceedings, in accordance with this PG.

**2.2.1.1. (U) Investigative Personnel and Analysts**

(U//~~FOUO~~) Investigative personnel handling, processing, and performing content reviews of DE (typically special agents [SA] and analysts) are responsible for:

- (U//~~FOUO~~) Conducting and/or directing the preview and/or review of DE content.
- (U//~~FOUO~~) Using approved DE tools for which approved training has been completed.

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

**2.2.1.2. (U) Computer Analysis and Response Team Technicians**

(U//~~FOUO~~) CART techs are responsible for imaging DE, using only approved tools and techniques.

**2.2.1.3. (U) Digital Extraction Technicians**

(U//~~FOUO~~) DExTs are responsible for:

- (U//~~FOUO~~) Processing images of DE to search, find, and extract items of interest from the DE within the defined scope of legal authority.
- (U//~~FOUO~~) Performing the DE functions authorized for CART techs as described above, if certified, and upon request. When performing these functions, the DExT must follow the protocols and limitations prescribed for that role.

**2.2.1.4. (U) Computer Analysis and Response Team Forensic Examiners**

(U//~~FOUO~~) CART FEs are responsible for:

- (U//~~FOUO~~) Performing any DE functions authorized for a CART tech or a DExT, upon request. When performing those functions, the CART FE must follow the protocols and limitations prescribed for those roles.
- (U//~~FOUO~~) Conducting and/or directing the forensic examination of DE, including:
  - (U//~~FOUO~~) [REDACTED]
  - (U//~~FOUO~~) [REDACTED]
  - (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED] in accordance with all provisions of this PG and relevant OTD/DEAS QA requirements.
- (U//~~FOUO~~) Providing [REDACTED] the execution of search warrants and previews/examinations of complex computer systems or situations.
- (U//~~FOUO~~) Providing on-scene consultations with investigators and prosecutors in the development of strategies for the seizure or on-scene imaging of digital media and equipment.

b7E -3, 4, 5

**2.2.1.5. (U//~~FOUO~~) Field Audio Video Program Forensic Analysts**

(U//~~FOUO~~) FAVP FAs are responsible for:

- (U//~~FOUO~~) Conducting and/or directing the content review of audio and video DE.
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

[REDACTED]

- (U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5

- (U//~~FOUO~~) [REDACTED]

**2.2.1.6. (U//~~FOUO~~) Computer Scientists-Field Operations**

(U) CS-FOs are responsible for:

- (U//~~FOUO~~) Performing any function related to DE that is carried out by a CART tech or DExT. When performing those functions, CS-FOs must follow the protocols and limitations prescribed for those roles.
- (U//~~FOUO~~) Supporting investigative and [REDACTED] personnel with computer science expertise in support of cases or investigations (e.g., assistance with interviews and searches), as authorized by this PG.
- (U//~~FOUO~~) Using [REDACTED] for all activities.

b7E -3, 4, 5

**2.2.1.7. (U) Regional Computer Forensics Laboratories Personnel**

(U//~~FOUO~~) RCFL personnel are responsible for performing duties as outlined in the memoranda of understanding (MOU) between their agencies and the FBI.

**2.2.2. (U) Federal Bureau of Investigation Headquarters**

**2.2.2.1. (U) Federal Bureau of Investigation Headquarters Operational Divisions**

(U//~~FOUO~~) The executive management of FBIHQ operational divisions is responsible for:

- (U//~~FOUO~~) Communicating the DE policies, procedures, and guidance set forth in this PG to personnel within their mission areas by posting a link to this PG on their respective division Intranet sites.
- (U//~~FOUO~~) Ensuring compliance with all matters identified in this PG.
- (U//~~FOUO~~) Monitoring compliance and reporting noncompliance in their respective mission areas in accordance with the guidance found in the *Domestic Investigations and Operations Guide (DIOG)*.

**2.2.2.1.1. (U) FBIHQ Operational Divisions Routinely Handling Digital Evidence**

**2.2.2.1.1.1. (U//~~FOUO~~)** [REDACTED]

(U//~~FOUO~~) [REDACTED] DExT personnel who are responsible for:

b7E -3, 4, 5, 6

- (U//~~FOUO~~) Serving as [REDACTED]
- (U//~~FOUO~~) [REDACTED]

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

- (U//~~FOUO~~) Following FBI DE protocols applicable to DExTs, as specified in this PG.
- (U//~~FOUO~~) [REDACTED]  
 [REDACTED]
- (U//~~FOUO~~) Providing copies of seized or otherwise legally obtained DE for upload into the [REDACTED] at the request of the case agent or FBIHQ program management unit and with the approval of OGC [REDACTED] b3 -1 b7E -2, 3, 4, 5, 6
- (U//~~FOUO~~) Providing copies of DE to IC partners, at the request of the case agent or FBIHQ program management unit and with the approval of [REDACTED]  
 [REDACTED]
- (U//~~FOUO~~) [REDACTED]  
 [REDACTED]

**2.2.2.1.1.2. (U//~~FOUO~~) Criminal Investigative Division (CID), Violent Crimes Against Children (VCAC) Section**

(U//~~FOUO~~) CID's VCAC Section provides [REDACTED] b7E -3, 4, 5  
 [REDACTED] abuse and exploitation of children that may be investigated under the jurisdiction and authority of the FBI. The OTD/DFAS/Digital Analysis and Research Center (DARC) [REDACTED]  
 [REDACTED]

(U//~~FOUO~~) VCAC manages several programs, including the Innocent Images National Initiative (IINI) and is responsible for establishing guidance for the handling of child pornography contraband for the IINI program.

**2.2.2.1.1.3. (U//~~FOUO~~) Operations Technology Division Digital Forensics and Analysis Section**

(U//~~FOUO~~) OTD's DFAS, in coordination with other FBI divisions, is responsible for:

- (U//~~FOUO~~) Creating and maintaining policies and procedures for the FBI's DE program, wherein such policies and procedures ensure compliance with governing legal authorities, regarding the manner in which DE is searched, processed, stored, accessed, used, and disseminated to maintain the integrity of the evidence and to ensure adherence to applicable privacy and civil liberties laws, policies, and regulations.
- (U//~~FOUO~~) Overseeing the FBI DE field subprograms, which include:
  - (U//~~FOUO~~) The Computer Analysis Response Team Forensic Examiner Subprogram.
  - (U//~~FOUO~~) The Digital Extraction Technician Subprogram.
  - (U//~~FOUO~~) The Computer Scientist-Field Operations Subprogram.
  - (U//~~FOUO~~) The Field Audio Video Program Subprogram.
  - (U//~~FOUO~~) The FBI Digital Evidence Laboratory (DEL) and Quality Assurance Program for DE.

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

- o (U//~~FOUO~~) The RCFL Subprogram.
- (U//~~FOUO~~) Providing the following capabilities and resources:
  - o (U//~~FOUO~~) Trained examiners who provide DE acquisition, preservation, processing, review, examination, presentation, and testimony.
  - o (U//~~FOUO~~) Trained personnel who provide advanced analysis capabilities for DE, including:
    - (U//~~FOUO~~) [REDACTED]
    - (U//~~FOUO~~) [REDACTED]
    - (U//~~FOUO~~) [REDACTED]
    - (U//~~FOUO~~) [REDACTED]
    - (U//~~FOUO~~) [REDACTED]
    - (U//~~FOUO~~) [REDACTED]
  - o (U//~~FOUO~~) Training, certification, and proficiency testing for personnel who process DE.
  - o (U//~~FOUO~~) [REDACTED]
  - o (U//~~FOUO~~) [REDACTED]
  - o (U//~~FOUO~~) [REDACTED]
  - o (U//~~FOUO~~) DE Help Desk [REDACTED]

b7E -3, 4, 5

b7E -3, 4, 5

**2.2.2.2. (U//~~FOUO~~) Office of the General Counsel**

(U//~~FOUO~~) An associate general counsel (AGC) from the Science and Technology Law Section (STLS) or an OGC supervisory attorney must, upon request, provide:

- Legal guidance to FBIHQ personnel on the handling, processing, and performing of content reviews of DE, in accordance with this PG.
- Legal policy guidance regarding the interpretation or application of this PG to FBIHQ, field office, and RCFL personnel.
- o Some RCFLs have [REDACTED]

b7E -3, 4, 5

**2.2.3. (U) FBI Field Offices**

**2.2.3.1. (U) FBI Field Office Management**

(U//~~FOUO~~) FBI field office management (i.e., assistant directors in charge [ADIC], special agents in charge [SAC], assistant special agents in charge [ASAC], and supervisory special agents [SSA]) are responsible for:

**UNCLASSIFIED//~~LES~~**  
**(U) Digital Evidence Policy Guide**

- (U//~~FOUO~~) Promoting and communicating DE policies.
- (U//~~FOUO~~) Ensuring compliance with this PG.
- (U//~~FOUO~~) Monitoring compliance and reporting noncompliance in their respective mission areas, in accordance with the DIOG.

**2.2.3.2. (U//~~FOUO~~) Evidence Control Technicians (ECT)**

(U//~~FOUO~~) Regarding DE, ECTs are responsible for:

- (U//~~FOUO~~) Properly storing, protecting, and tracking DE, as described in subsection 4.2.4.5, of this PG.
- (U//~~FOUO~~) Properly packaging and shipping DE, as necessary, as described in subsections 4.2.4.6. and 4.2.4.6.1, of this PG.

**2.2.3.3. (U) Chief Division Counsels**

CDCs must, upon request, provide legal guidance regarding the handling, processing, and the performing of content reviews of DE, in accordance with this PG. CDCs' responsibilities with regard to evidence may be delegated to an ADC or an LA.

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

### **3. (U) Policies**

---

(U//~~FOUO~~) This PG establishes and consolidates the policies and procedures for the proper handling, reviewing, and processing of DE for the FBI, whether it is seized, received, or otherwise legally obtained. DE is data that is stored or transmitted in binary form and is obtained with the intent to assist in proving or disproving a matter at issue in a case or an investigation. Digital evidence includes binary data stored on magnetic, optical, or mechanical storage devices, including, but not limited to, integrated circuits, microcontrollers, chips, tapes, computers, cell phones, CDs/DVDs, flash drives, RAM, magneto optical cartridges, USB micro storage devices (commonly known as "thumb drives"), DVRs, or other electronic devices that store or process data digitally. The OTD DFAS is responsible for the FBI's Digital Evidence Program and establishing DE policies.

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

## **4. (U) Procedures and Processes**

### **4.1. (U//~~FOUO~~) Forensic Program Compliance Within the FBI**

(U//~~FOUO~~) All DE forensic programs and subprograms conducted in FBI space must fully comply with FBI forensic policies, procedures, and requirements, as set by OTD/DFAS, and must be under the direct and immediate control and supervision of the OTD/DFAS unless prior written concurrence of the assistant director (AD), OTD or his or her designee is obtained.

### **4.2. (U) Digital Evidence Handling**

(U//~~FOUO~~) This section sets forth policies and procedures related to the handling of DE for all personnel working for or with the FBI, including investigative and technical personnel, ECTs, CART techs, DEXTs, CART FEs, CSs, DFAS technical experts, FAVP FAs, RCFL personnel, and other personnel who encounter DE.

#### **4.2.1. (U) Personnel Authorized to Handle Digital Evidence**

(U//~~FOUO~~) Level one and above personnel (as defined in Figure 1) are authorized to seize, image, and transport DE, provided that they act within the scope of their training and certifications. FBI personnel must also be trained and/or certified in accordance with OTD/DFAS policies and procedures and follow all applicable protocols before processing DE, including making copies or images of DE.

#### **4.2.2. (U) Presearch Considerations**

##### **4.2.2.1. (U//~~FOUO~~) Legal Review**

(U//~~FOUO~~) FBIHQ and field office personnel must ensure that the seizure and examination of DE strictly adheres to the procedures listed in this PG. Personnel handling DE may request CDC or OGC legal review of DE-related search warrants and subpoenas, as applicable [REDACTED] b3 -1 b7E -2, 3, 4, 5, 6

Field office CDCs and OGC are also available to provide assistance in drafting search warrants or subpoenas for seizing or searching DE.

#### **4.2.3. (U) Timeframe for Warrants Involving Digital Evidence**

(U//~~FOUO~~) Although Rule 41(e)(2)(A) does not place a specific time limit on off-site copying or review of electronic storage media, some judicial districts place specific limits on the amount of time permitted for off-site review. Case agents should consult with their CDCs or OGC [REDACTED] b7E -3, 4, 5, 6 there are questions pertaining to time permitted for examination.

#### **4.2.4. (U) Consent Searches for Digital Evidence**

(U//~~FOUO~~) Whenever possible, written consent must be obtained from the consenting party and documented on an FD-26, "Consent to Search" or an FD-941, "Consent to Search Computer(s)." However, this does not mean that oral consent is not valid. The case agent must, when relying on oral consent, appropriately document the oral consent on an FD-302, "Form for Reporting Information That May Become the Subject of Testimony."

(U//~~FOUO~~) In consent cases, case agents should ensure that [REDACTED] b7E -3, 4, 5

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

(U//~~FOUO~~) If consent is terminated, the case agent must immediately contact personnel processing the DE and notify them of the revocation of consent. Once consent is withdrawn, any imaging not completed must be terminated. The case agent should also promptly contact the CDC or OGC for advice on how to proceed with searching any completed or partial images made prior to the revocation.

**4.2.4.1. (U) Requesting Local Field Office Assistance**

(U//~~FOUO~~) DExT personnel may provide on-scene support for routine DE handling and processing in accordance with the procedures outlined in this PG. DExT support may be requested through, and in coordination with, the appropriate squad supervisor(s).

(U//~~FOUO~~) FBI case agents who require search and seizure assistance and/or examinations of DE must contact their field office CART supervisors, CART coordinators, or other CART personnel.

(U//~~FOUO~~) Case agents must submit requests for DE assistance to CART personnel via electronic communication (EC) or, where available, an automated request through the approved OTD/DFAS Intranet site or an RCFL service request form. All service requests must include:

- (U//~~FOUO~~) The universal case file number (UCFN) (case identification number [ID]).
- (U//~~FOUO~~) The case title.
- (U//~~FOUO~~) The specific request.
- (U//~~FOUO~~) The description of legal authority.

**4.2.4.2. (U) Requests Involving Multiple Locations**

(U//~~FOUO~~) Case agents must coordinate, in advance, any DE service requests involving multiple field offices with the CART supervisors or coordinators in their divisions, as well as with the other applicable divisions. If further assistance is required, CART supervisors or coordinators should work with the OTD/DFAS/Digital Evidence Field Operations Unit (DEFU).

**4.2.4.3. (U) Providing [REDACTED] Technical Assistance in Digital Evidence Cases** b7E -3, 4, 5

(U//~~FOUO~~) The FBI provides DE forensic services through [REDACTED]

(U//~~FOUO~~) Pursuant to Title 28 Code of Federal Regulations (CFR) Section (§) 0.85(g) and the DIOG, the FBI DEL and RCFLs are authorized to provide, without cost, technical and scientific assistance, including expert testimony in federal or local courts, to all duly constituted law enforcement agencies, other organizational units of the Department of Justice, and other federal agencies. Under this authority, the FBI DEL and RCFLs may also provide technical and scientific assistance, including expert testimony, [REDACTED] b7E -3, 4, 5

(U//~~FOUO~~) The FBI DEL consists of the following units, all of which are components of the OTD/DFAS Forensic Analysis Unit (FAU), Forensic Support Unit (FSU), and the Forensic Audio, Video and Image Analysis Unit (FAVIAU). The DFAS forensic examiners (see subsection 2.1, "Digital Evidence Roles") that comprise the DEL consist of CART-FEs, CART FETs and FAVIAU examiners.

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

(U//~~FOUO~~) The following OTD/DFAS units are not components of the FBI DEL: (1) the

b7E -3, 4, 5, 6

[REDACTED]  
 [REDACTED] Field office  
 CART assets and laboratories are not part of the FBI DEL. Although RCFLs follow the FBI DEL's Quality Assurance Program, each RCFL is an individually accredited lab, independent from other RCFLs and the FBI DEL.

(U//~~FOUO~~) In accordance with the DIOG, the provision of routine forensic analysis and examination of submitted evidence is considered technical and scientific support. Routine forensic analysis and examination of evidence performed by the FBI DEL, RCFLs, or CART personnel in field offices is not considered expert investigative assistance (as defined in the DIOG), even if those components are providing expert witness testimony in connection with the support.

**4.2.4.3.1. (U) Expert Investigative Assistance in Digital Evidence Cases**

(U//~~FOUO~~) FBI personnel, particularly approving officials, must be careful to review

b3 -1

b7E -2, 3, 4, 5

[REDACTED]  
 [REDACTED] see the  
DIOG.

(U//~~FOUO~~) During the course of providing either

b3 -1

b7E -2, 3, 4, 5, 6

[REDACTED]

**4.2.4.3.2. (U) Requests for**

[REDACTED] the Digital Evidence Laboratory or Regional  
 Computer Forensics Laboratories

(U//~~FOUO~~) FBI components that are not part of the FBI DEL or RCFLs may only provide technical assistance pursuant to Attorney General Order 2954-2008 and the DIOG.

(U//~~FOUO~~) Requests for [REDACTED] than the  
 FBI DEL or RCFLs must be processed and handled in accordance with the DIOG and the

[REDACTED], as applicable.

b3 -1

b7E -2, 3, 4, 5

(U//~~FOUO~~)

[REDACTED]

**4.2.4.3.3.**

(U)

[REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

**4.2.4.3.3.1. (U) Requests to the FBI Digital Evidence Laboratory**

(U//~~FOUO~~) Requests submitted to the DEL for [REDACTED] b3 -1  
b7E -2, 3, 4, 5

[REDACTED]

(U//~~FOUO~~) [REDACTED] b3 -1  
b7E -2, 3, 4, 5

[REDACTED]

(U//~~FOUO~~) [REDACTED] b3 -1  
b7E -2, 3, 4, 5

[REDACTED]

(U//~~FOUO~~) [REDACTED] b3 -1  
b7E -2, 3, 4, 5

[REDACTED]

(U//~~FOUO~~) [REDACTED]

[REDACTED]

(U//~~FOUO~~) [REDACTED] b3 -1  
b7E -2, 3, 4, 5

[REDACTED]

(U//~~FOUO~~) [REDACTED]

[REDACTED]

**4.2.4.3.3.2. (U) Requests for Regional Computer Forensic Laboratory Support**

(U//~~FOUO~~) Requests for RCFL DE support from [REDACTED] will be handled in accordance b7E -3, 4, 5  
with the applicable MOU governing the RCFL concerned, provided that the MOU is consistent  
with this PG.

(U//~~FOUO~~) Because the authority to provide this support is under 28 CFR § 0.85(g), a federal  
nexus is not required, and such services must be provided at no cost to the requesting agency.

RCFLs may not provide [REDACTED] All b3 -1  
such requests must be referred to the FBI DEL. b7E -2, 3, 4, 5

(U//~~FOUO~~) [REDACTED]  
[REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

[REDACTED]

b3 -1  
b7E -2, 3, 4, 5

(U//~~FOUO~~) The processing of the DE and dissemination of materials and information pertaining to the technical assistance by RCFLs must be in accordance with this PG.

(U//~~FOUO~~) RCFLs will track all service requests and disseminate information to [REDACTED]

b3 -1  
b7E -2, 3, 4, 5

[REDACTED]

**4.2.4.3.4. (U//~~FOUO~~) Requests for the Use of [REDACTED]**

(U//~~FOUO~~) Requests for the use of FBI or other [REDACTED] in criminal cases require the review and recommendation of OGC [REDACTED] and the DOJ's Criminal Division, as well [REDACTED] approval by the DAG. See the DAG memorandum entitled [REDACTED],

b3 -1  
b7E -2, 3, 4, 5, 6

(U//~~FOUO~~) Requests for the use of [REDACTED]

(U//~~FOUO~~) The dissemination of protected information must be in accordance with the DIOG.

(U//~~FOUO~~) Prior to the approval of a request, assurances must be obtained from the requesting agency and the chief prosecutor for the applicable jurisdiction that representatives of the requesting agency will not disclose [REDACTED] in court, through pretrial motions, discovery, or other means, or through any federal or state freedom of information legislation or similar law, or otherwise disclose to the media or public, without the prior written consent of the Director, FBI, or his or her designee. The requesting agency and the chief prosecutorial official will also acknowledge that they are receiving the requested technical assistance expressly conditioned on the fact that they are subject to the nondisclosure provisions governing FBI information, as set forth in 28 CFR §§ 16.22, 16.24, and 16.26, as well FBI policies on the protection, use, and [REDACTED]

b7E -3, 4, 5

**4.2.4.4. (U) Digital Evidence and Evidence Control Facilities (ECF)**

(U//~~FOUO~~) The original DE seized at a search site must be transported securely to the FBI field office or RCFL site and, after processing and examination, be placed, as appropriate, in an FBI or RCFL ECF.

**4.2.4.5. (U) Digital Evidence Storage**

(U//~~FOUO~~) DE must be stored and secured and/or sealed to prevent data or evidentiary loss, cross-transfer contamination, or other deleterious changes.

**UNCLASSIFIED//~~LES~~**  
**(U) Digital Evidence Policy Guide**

**4.2.4.6. (U) Shipping Digital Evidence**

(U//~~FOUO~~) Shipping of DE from field offices to FBIHQ or RCFLs must be handled through an FBI ECF.

**4.2.4.6.1. (U) Shipping Digital Evidence to the Computer Analysis and Response Team**

(U//~~FOUO~~) When it has been determined that DE needs to be shipped either to another field office CART FE or to the OTD/DFAS, the DE must be processed through the field office's ECT. The ECT must ensure that the DE is packaged securely and that proper chain-of-custody procedures are followed. For assistance in packing DE for shipping, the case agent should contact the ECT in his or her field office. The DE must be accompanied by an EC explaining the shipment.

**4.2.4.7. (U) Transferring a Working Copy of FBI Digital Evidence to [REDACTED]**

b7E -3, 4, 5, 6

(U//~~FOUO~~) Case agents may submit working copies of [REDACTED]

[REDACTED] Submission may be accomplished by completing a transmission request EC in Sentinel, and providing a working copy of the DE to [REDACTED]

**4.3. (U) Digital Evidence Processing**

**4.3.1. (U) Imaging**

(U//~~FOUO~~) Imaging is the act of making a [REDACTED] copy of the original DE to serve as an accurate reproduction of the original DE. Only certified DE personnel must perform imaging. Certified DE personnel (i.e., CART FEs, CART techs, DExTs, and FAVP FAs) must follow standard CART procedures and QA requirements when imaging DE. Specific procedures for imaging digital media are detailed in the [REDACTED]

b7E -3, 4, 5

**4.3.2. (U) [REDACTED]**

b7E -3, 4, 5

(U//~~FOUO~~) [REDACTED]

**4.3.3. (U) [REDACTED]**

b7E -3, 4, 5, 6

(U//~~FOUO~~) [REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

b7E -3, 4, 5, 6

## 4.3.3.1. (U) [REDACTED]

(U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5, 6

## 4.3.4. (U) Performing Content Reviews

(U//~~FOUO~~) Investigative personnel can review DE for content after the DE has been processed by an authorized method. This review may be conducted using such methods as [REDACTED]

b7E -3, 4, 5

## 4.3.4.1. (U) Scope and the Performing Content Review

(U//~~FOUO~~) When searching DE pursuant to legal authority, an agent is authorized to seize only items specified in, and responsive to, the authority, absent an independent legal basis under which materials can be seized or retained.<sup>1</sup>

(U//~~FOUO~~) When searching DE pursuant to a criminal warrant, the warrant permits only a search for evidence of a specific, enumerated crime or crimes; therefore, agents may only seize items that are within the bounds of the warrant, commonly known as the "scope" of the warrant.

(U//~~FOUO~~) When searching DE [REDACTED]

b3 -1

b7E -2, 3, 4, 5

[REDACTED] the government must not exceed the scope authorized in the order. Questions regarding the authorized scope of a search should be directed to the servicing legal counsel (CDC/ADC or OGC).

4.3.4.2. (U//~~FOUO~~) Scope Issues in Consent Cases

(U//~~FOUO~~) Where consent is the legal authority for a search of DE, the ability of FBI personnel to review the digital evidence is bound by the terms of the consent provided. Consenting individuals may impose binding limitations on the areas or items that may be searched (e.g., specific rooms of a house or specific files or folders on a computer), either orally or on the written consent form.

<sup>1</sup>(U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

**4.3.4.3. (U//~~FOUO~~) Search Protocols for Digital Evidence**

(U//~~FOUO~~) When examining or reviewing DE, all FBI personnel must observe all restrictions written into warrants, including local protocols attached to any warrants. Questions regarding such provisions should be directed to the servicing legal counsel (CDC/ADC or OGC).

**4.3.4.4. (U) Self-Service Kiosks**

(U//~~FOUO~~) Self-service kiosks are provided in most field offices. In addition, portable kiosk kits are available in many FBI resident agencies (RA). Investigative personnel must use the kiosks, when reasonably available, to automatically process supported DE types, unless otherwise directed by CART personnel.

(U//~~FOUO~~) [REDACTED] b7E -3, 4, 5  
[REDACTED]  
[REDACTED] self-paced or hands-on training is required.

(U//~~FOUO~~) [REDACTED]  
[REDACTED]  
[REDACTED] self-paced or hands-on training is required.

**4.3.4.5. (U) Authorization for Performing Content Reviews**

(U//~~FOUO~~) Performing content reviews is authorized only after DE is processed by authorized personnel (i.e., CART FEs, CART techs, DExTs, or FAVP FAs), with the following exceptions:

- (U//~~FOUO~~) [REDACTED] approved by OTD/DFAS are utilized
- (U//~~FOUO~~) Preview [REDACTED] OTD/DFAS policies
- (U//~~FOUO~~) Preview by RCFLs or CART field office facilities, in accordance with OTD/DFAS policies b7E -3, 4, 5
- (U//~~FOUO~~) The use of self-service kiosks for [REDACTED]

(U//~~FOUO~~) Performing content reviews of original DE is prohibited by those not trained and authorized by OTD

**4.3.4.6. (U//~~FOUO~~) [REDACTED]**  
(U//~~FOUO~~) [REDACTED]  
[REDACTED] within the scope of the legal authority. The information obtained through [REDACTED] b7E -3, 4, 5  
[REDACTED]

**4.3.4.7. (U) [REDACTED]** b7E -3, 4, 5

(U//~~FOUO~~) [REDACTED]  
[REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

b7E -3, 4, 5

#### 4.3.4.8. (U) Content Review Tools

(U//~~FOUO~~) All DE content review tools used by personnel working for or with the FBI or RCFL must be legally obtained and used in accordance with the limitations in the licensing agreement, unless a legal exception applies (e.g., fair use or specific guidance in the legal authority) and the reviewer has coordinated with his or her CDC or OGC. If proprietary software is seized with the data, it may be used to view the data from the investigation.

#### 4.3.5. (U) Documenting Review of DE

(U//~~FOUO~~) FBI personnel must document all reviews and searches of DE from the point of the receipt of DE through completion of the search, including any identification of evidence that falls within the scope of the warrant or is identified as [REDACTED]. The [REDACTED] documentation must be serialized to the investigative case file. Such documentation must identify, at a minimum, the general nature and manner in which the search of the media was conducted, major steps taken during the search, and forensic tools employed during the search. b3 -1 b7E -2, 3, 4, 5

(U//~~FOUO~~) Undocumented, "off-the-record" searches or reviews of DE are not permitted. The above documentation requirement does not apply to searches of [REDACTED] (see subsection 4.3.5.6 of this PG for a definition of a [REDACTED]).

(U//~~FOUO~~) The four categories of reports are:

1. (U//~~FOUO~~) Content review report: reports factual information resulting from the review of DE.
2. (U//~~FOUO~~) DExT report: reports factual information resulting from the [REDACTED] b7E -3, 4, 5
3. (U//~~FOUO~~) Report of examination: reports the results of an examination performed by a certified examiner or other technical expert, usually with information regarding advanced analysis or opinions.
4. (U//~~FOUO~~) [REDACTED] b3 -1 b7E -2, 3, 4, 5

#### 4.3.5.1. (U) Content Review Report

(U//~~FOUO~~) A content review report is a factual report of investigative findings resulting from the review of original, master, or [REDACTED] of the DE. Because [REDACTED] b7E -3, 4, 5

The report details who performed the review, when it was performed, what was reviewed and found, and where it was found. A content review report may be documented by completing an FD-302, "Form for Reporting Information That May Become the Subject of Testimony."

Content review reports must be serialized into the investigative file. A content review report must contain, at a minimum, the following information:

- (U//~~FOUO~~) Name and contact information of the reviewer.

**UNCLASSIFIED//~~LES~~**  
**(U) Digital Evidence Policy Guide**

- (U//~~FOUO~~) Description of the working copy reviewed, including case number and original DE description.
- (U//~~FOUO~~) The physical location of where the review was completed (i.e., location of the reviewer).
- (U//~~FOUO~~) The date of the report.
- (U//~~FOUO~~) The methodology and basis for their conclusion that the [REDACTED] b7E -3, 4, 5  
[REDACTED]
- (U//~~FOUO~~) Report of the responsive content found, including [REDACTED] b7E -3, 4, 5  
[REDACTED]

(U//~~FOUO~~) All FBI personnel must fully and officially document in the content review report any other individuals who provided substantive assistance (as opposed to purely technical assistance, [REDACTED]) b7E -3, 4, 5

(U//~~FOUO~~) A content review report must contain only factual information and must not contain expert opinions related to the DE, other than those expressly permitted in this section and considered to be advanced technical analysis (see subsection 2.1, Figure 1).

**4.3.5.2. (U) Digital Extraction Technician Report**

(U//~~FOUO~~) A DExT report is a factual report of [REDACTED] details who performed the b7E -3, 4, 5 work, when it was performed, what was reviewed and found, and where it was found. DExT work may be documented by completing an FD-302, "Form for Reporting Information That May Become the Subject of Testimony," in accordance with the [REDACTED]

[REDACTED] prescribed by OTD/DFAS. DExT reports must be serialized into the investigative case file and must contain a minimum of the following information or provide a reference to where the information may be found:

- (U//~~FOUO~~) Name and contact information of the DExT.
- (U//~~FOUO~~) Case identification.
- (U//~~FOUO~~) Name of requestor and specifically what was requested.
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description.

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

- (U//~~FOUO~~) Physical location of where the review was completed (i.e., location/address of the reviewer).
- (U//~~FOUO~~) Date of the report.
- (U//~~FOUO~~) List of procedures performed.
- (U//~~FOUO~~) What was searched for and what items of investigative importance were found (including negative search results, when applicable).
- (U//~~FOUO~~) Where the DExT is a case agent or investigator and is reviewing or conducting an [redacted] on his or her own case evidence, the methodology and basis for his or her conclusion that the [redacted] b7E -3, 4, 5

- (U//~~FOUO~~) Report of the responsive content found, including [redacted]
- (U//~~FOUO~~) [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted] b7E -3, 4, 5
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) What was targeted during the search and, if applicable, the order in which items were targeted [redacted] b7E -3, 4, 5

(U//~~FOUO~~) All DExTs must fully and officially document in the DExT report any other individuals who provided substantive assistance with the [redacted] b7E -3, 4, 5

(U//~~FOUO~~) A DExT report must contain only factual information and must not contain expert opinions related to the DE, other than those expressly permitted in this section and considered to be advanced technical analysis (see subsection 2.1, Figure 1).

(U//~~FOUO~~) If the DExT is an FBI investigative asset (e.g., an SA or an intelligence analyst [IA]) and is performing a content review and DExT review simultaneously in his or her own case, only a DExT report is required.

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

#### 4.3.5.3. (U) Report of Examination

(U//~~FOUO~~) A report of examination is used to document the results of [REDACTED] and must be serialized into the investigative file. For CART FEs and forensic audio, video, and image examiners, the report of examination is required to be documented by completing all fields in a [REDACTED] [REDACTED] [REDACTED] may use other reporting formats approved by OTD/DFAS. Reports of examination must be serialized into the investigative case file and must contain a minimum of the following information or provide a reference to where the information may be found. If relying on the reference provision, all references must accompany the report of examination provided to the defendant during discovery.

b7E -3, 4, 5

- (U//~~FOUO~~) Name and contact information of the examiner
- (U//~~FOUO~~) Case identification
- (U//~~FOUO~~) Name of requestor and specifically what was requested
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description
- (U//~~FOUO~~) Physical location of where the review was completed (i.e., location/address of the reviewer)
- (U//~~FOUO~~) Date of the report
- (U//~~FOUO~~) Procedures performed, which may include the following:
  - o [REDACTED]
  - o Types of files targeted ([REDACTED])
  - o The order in which items were searched (if applicable)

b7E -3, 4, 5

- (U//~~FOUO~~) Items searched for and items found of investigative importance, including negative search results, when applicable
- (U//~~FOUO~~) Report of the content found, [REDACTED]

b7E -3, 4, 5

- (U//~~FOUO~~) [REDACTED]

(U//~~FOUO~~) All FBI personnel must also fully and officially document in the report of examination whenever they received substantive assistance from another individual during the examination or review process (not including help-desk-type assistance), including [REDACTED]

b7E -3, 4, 5

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

[REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) Frequently, in the course of the investigation or during trial preparation, an examiner will be asked to perform additional analysis of the DE. If this occurs, the examiner must file a supplemental report of examination, in accordance with the requirements above, to document fully the additional analysis requested, in accordance with the Federal Rules of Criminal Procedure Rule 16.

4.3.5.4. (U) [REDACTED] Reports

b7E 3, 4, 5, 6

(U//~~FOUO~~) [REDACTED]  
[REDACTED]

[REDACTED] Intelligence reports must be serialized into the investigative case file and must contain the following information, if applicable:

- (U//~~FOUO~~) Case identification
- (U//~~FOUO~~) Name of requestor and specifically what he or she requested
- (U//~~FOUO~~) Description of the working copy processed, including case number and original DE description
- (U//~~FOUO~~) Physical location of where the review was completed (i.e., location of the reviewer)
- (U//~~FOUO~~) Date of the report
- (U//~~FOUO~~) List of procedures performed
- (U//~~FOUO~~) What was searched for and what items of investigative importance were found
- (U//~~FOUO~~) Report of the responsive content found, including identifying the [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) What was targeted during the search and, if applicable, the order in which items were targeted [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) [REDACTED]  
report, any other individuals who provided substantive assistance with the [REDACTED] (not including help desk-type assistance) [REDACTED] must, at a minimum, include who assisted them during the processing and, if applicable, who

b7E -3, 4, 5, 6

[REDACTED]  
[REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

(U//~~FOUO~~) [redacted] report must contain only factual information and must not contain expert opinions related to the DE that would fall within the description of advanced technical analysis (see subsection 2.1, Figure 1). b7E -3, 4, 5

**4.3.5.5. (U) Testifying Regarding Review of Digital Evidence**

(U//~~FOUO~~) All personnel who handle DE must be prepared to testify concerning their findings and actions when seizing, handling, previewing, processing, or reviewing DE. To facilitate accurate and complete testimony, documentation must be as detailed and extensive as necessary to recall all key aspects of their activities.

**4.3.5.6. (U) Retaining Results of Review**

(U//~~FOUO~~) After the DE is reviewed and/or examined, the set of data that (1) is determined to be within the scope of the legal authority, (2) is relevant, and (3) is probative or exculpatory must be

[redacted] b7E -3, 4, 5

(U//~~FOUO~~) The results of a content review or an examination must be [redacted]

[redacted]

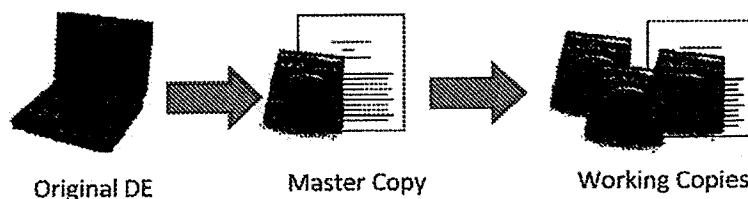
(U//~~FOUO~~) The [redacted] may be charged out by the case agent or any other party authorized by the case agent or the case agent's chain of command.

**4.3.6. (U) Copies**

**4.3.6.1. (U) Original Digital Evidence vs. Master Copy vs. Working Copy vs. [redacted]** b7E -3, 4, 5

(U//~~FOUO~~) Digital evidence is unique in that it can, in many cases, be duplicated or imaged

[redacted]



[redacted] b7E -3, 4, 5

**Figure 2. (U//~~FOUO~~) Digital Evidence Copies**

(U//~~FOUO~~) Original DE: DE seized at a search scene or otherwise lawfully obtained and stored in an ECF. If another agency transmits image copies on digital media without the original device accompanying it, the original copy received is the original DE copy.

(U//~~FOUO~~) With the exception of contraband, items subject to statutory forfeiture or instrumentalities of a crime, original DE may be returned to its rightful owners when all criminal proceedings have terminated and the CDC and AUSA/prosecutor have concurred. FBI personnel who are directed to return original DE prior to the conclusion of the trial should contact their

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

CDCs/ADCs and OGC [redacted] to ensure that the proper stipulations are entered into to prevent challenges to authenticity after return of the media. b7E -3, 4, 5, 6

(U//~~FOUO~~) If the original DE contains contraband and the device was not forfeited, FBI personnel must not destroy the entire computer. Instead, the hard drive with the contraband must be removed and physically destroyed or the contents removed in a manner that would preclude recovery.

(U//~~FOUO~~) Master copy: the one required copy of DE that is stored on media to be retained and logged on an FD-1004, "Federal Bureau of Investigation Evidence Chain of Custody" form. [redacted] b7E -3, 4, 5

[redacted]

(U//~~FOUO~~) Working copy [redacted]

[redacted]

(U//~~FOUO~~) Working copies [redacted]

b7E -3, 4, 5

[redacted]

(U//~~FOUO~~) Restrictions on the tracking, dissemination, and copying of [redacted]

b7E -3, 4, 5

[redacted]

(U//~~FOUO~~) A copy of the original legal authority should be maintained with each working copy of the DE [redacted]

[redacted]

b7E -3, 4, 5

(U//~~FOUO~~) [redacted]

[redacted]

(U//~~FOUO~~) It is impossible to guarantee that [redacted]

b7E -3, 4, 5

[redacted]

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

[REDACTED] b7E -3, 4, 5

**4.3.6.2. (U) Controlling Master Copies**

(U//~~FOUO~~) All master copies must be saved [REDACTED]

[REDACTED] The original legal authority must be reviewed prior to making any copies [REDACTED]

b3 -1  
b7E -2, 3, 4, 5

(U//~~FOUO~~) Master copies may be in two forms:

1. (U//~~FOUO~~) [REDACTED] b7E -3, 4, 5

2. (U//~~FOUO~~) [REDACTED]

(U//~~FOUO~~) DE that is received in an ECF and is marked "master copy" must be assigned a new 1B number and given a new bar code, as applicable. In the description field, the ECT must include the original 1B number from which the DE was derived.

(U//~~FOUO~~) To ensure the integrity of the master copy and to prevent unauthorized copies from being disseminated, a master copy may only be charged out by DE personnel (i.e., CART FEs, CART techs, DEXTs, and FAVP FAs).

**4.3.6.3. (U) Protecting Original Evidence or Master Copies**

(U//~~FOUO~~) Unless it is not technically possible, examinations or reviews of DE [REDACTED]

b7E -3, 4, 5

**4.3.6.4. (U) Previews of Original Evidence**

(U//~~FOUO~~) In accordance with this PG, FBI personnel may conduct previews of original DE. In these cases, personnel may only conduct previews in accordance with procedures approved by OTD/DFAS [REDACTED]

b7E -3, 4, 5

**4.3.6.5. (U) Disseminating [REDACTED]**

(U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

[REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) All FBI personnel receiving requests for [REDACTED] must first look to the language of the relevant legal authority to determine whether dissemination of images or copies of DE is authorized by the court order for the stated purpose. [REDACTED]

[REDACTED] FBI personnel may provide a [REDACTED] of that legal authority is included in the investigative case file and if the provision of [REDACTED] is documented as outlined in this section.

(U//~~FOUO~~) [REDACTED] FBI personnel may disseminate, with OGC's approval, [REDACTED]

b3 -1

b7E -2, 3, 4, 5

[REDACTED] Such dissemination must be documented in the case file, as outlined in this section.

(U//~~FOUO~~) Only certified DE personnel (i.e., CART FEs, CART techs, DExTs, FAVP FAs, and OTD/DFAS technical experts) are allowed to create media of working copies. All copies made after (or from) the master copy, [REDACTED] are required to be labeled as working copies, except as noted.

b7E -3, 4, 5

(U//~~FOUO~~) Case agents must document the dissemination of working copies for tracking purposes in the case file. The case agent is required to document his or her name, the number of working copies provided, the recipient [REDACTED] the UCFN or file number, the evidence number, who requested the working copy on what date and at what time, and the purpose for the working copy.

(U//~~FOUO~~) At the discretion of the case agent or the case agent's supervisor, working copies may be submitted to an ECF for chain-of-custody tracking. In addition, the creation of the copy must be documented by the certified DE personnel in the examination file or DExT report, as applicable.

(U//~~FOUO~~) The case agent or FBIHQ program manager may disseminate working copies of DE to [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) Because DE may contain contraband, personally identifiable information (PII), privileged files or other legally protected information, [REDACTED]

b7E -3, 4, 5

[REDACTED] must be appropriately marked [REDACTED]

#### 4.3.6.5.1. (U) Copies of Digital Evidence for the United States Attorney's Office

(U//~~FOUO~~) Only [REDACTED] of DE may be provided to USAOs, unless otherwise authorized by this section. To obtain a working copy of DE, the USAO must request the copy in writing and explain the purpose of obtaining an image or a working copy of the media. The request must include whether the USAO intends to further disseminate the media and, if so, to whom and for what purpose (e.g., to facilitate an examination or review by non-FBI personnel). In this event, the request must be handled as [REDACTED] request or reexamination request (as

b7E -3, 4, 5

**UNCLASSIFIED//~~LES~~**  
**(U) Digital Evidence Policy Guide**

outlined below). When reviewing such a request, FBI personnel may only comply when the following requirements have been met:

- (U//~~FOUO~~) The court order clearly authorizes such a dissemination would occur under the relevant circumstances in the underlying application for the legal authority.
- (U//~~FOUO~~) The affiant advised the court that such a dissemination would occur under the relevant circumstances in the underlying application for the legal authority.
- (U//~~FOUO~~) The case agent, in consultation with his or her CDC and OGC [REDACTED] b7E -3, 4, 5, 6 determines that such a dissemination is otherwise authorized.

(U//~~FOUO~~) Statements in search warrant affidavits or other applications or orders ambiguously authorizing the search and seizure of media by “government personnel,” or similar language, are insufficient to meet the above requirements. For the purposes of this section, “government personnel” does not include AUSAs, paralegals, or other personnel in a USAO, nor does it include trial attorneys, paralegals, or other personnel in DOJ who do not meet the definition of a “federal law enforcement officer” authorized to execute a search warrant in Rule 41(a)(2)(C), Federal Rules of Criminal Procedure.

(U//~~FOUO~~) The above restriction applies in circumstances where the judicial order authorizes the ultimate seizure of only a subset of data that exists on the media initially seized [REDACTED] b7E -3, 4, 5

(U//~~FOUO~~) If FBI personnel are requested to provide such copies or otherwise facilitate such a transfer, they should inform the UC of the Forensic Support Unit, their squad supervisors, and their CDCs. When personnel comply with such a request pursuant to the procedures described above, they must clearly document the details of the request and compliance with the above requirements in the agent's investigative case file and, if applicable, any digital evidence examination file. FBI personnel must also comply with any other relevant policies or procedures, such as the need to obtain the approval of the AD of OTD for a second examination of digital evidence.

#### **4.3.6.5.2. (U) Discovery Requests**

(U//~~FOUO~~) Discovery requests must be accommodated following applicable laws.

(U//~~FOUO~~) The dissemination of working copies of DE to the defense to facilitate a discovery request is the case agent's responsibility. Prior to disseminating working copies for discovery, the case agent must protect PII (e.g., social security numbers, telephone numbers, bank account numbers, and medical records) in accordance with federal law. The case agent must document the provision of discovery copies in the investigative case file.

##### **4.3.6.5.2.1. (U) Providing Digital Evidence with No Contraband**

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

(U//~~FOUO~~) The party requesting discovery must either supply suitable (size, quantity, and type) media for duplication of the data subject to disclosure or make arrangements for replacement of expended media.

(U//~~FOUO~~) Copies prepared pursuant to a discovery request are typically [REDACTED] b7E -3, 4, 5 and must be verified as appropriate for disclosure by the case agent, in consultation with the AUSA, prior to release as discovery. In accordance with DOJ e-discovery guidance, the FBI is under no obligation to create [REDACTED] for discovery. The FBI does not provide this service due to the administrative burden that results and the inability [REDACTED]

**4.3.6.5.2.2. (U) Requests for Digital Evidence Containing Contraband**

(U//~~FOUO~~) When discovery is requested of material containing contraband (e.g., child pornography), the FBI must follow the procedures outlined in Title 18 United States Code (U.S.C.) Section (§) 3509(m), the Adam Walsh Child Protection and Safety Act (the Act). Pursuant to the Act, the FBI is required to make reasonable accommodations, frequently called Adam Walsh rooms, specifically configured for these types of reviews, for the defense to have access to such material in an FBI facility. Reasonable accommodations include access to the government-controlled facility during normal business hours, access to telephones, access to the Internet, and access to printers. Defense experts may make special, advance arrangements to use the facility outside of normal business hours; however, this must be based on a compelling need and will not be done as a matter of routine practice due to the fiscal and workforce expenses to the FBI.

(U//~~FOUO~~) Defense experts may use their own computers and tools to conduct an analysis; however, they must be notified in advance that any digital media entering the government facility must be forensically wiped prior to their departure in order to ensure FBI compliance with the requirements of the Adam Walsh Act. If the field office does not have a segregated Adam Walsh room, the chief security officer (CSO) must be notified in advance that defense experts may have laptops or other portable electronic devices to support the discovery. The case agent must coordinate with the CSO for appropriate access. If the defense expert requires more than one session to complete the exam, reasonable accommodation may also include that the FBI provide either a lockable, private space within the government-controlled facility or a locking safe in which the defense expert may store his or her tools and equipment when away from the room. These measures ensure attorney-client privilege and work products are not exposed accidentally to the government.

(U//~~FOUO~~) If a defense expert requests to take any materials generated during the examination from the government-controlled facility, all materials must be reviewed to ensure that no contraband, law enforcement sensitive (LES, or classified materials have been included. If the defense expert objects to this review, CART personnel must notify their supervisor(s) and CDCs/ADCs or OGC [REDACTED] for input and assistance in resolving the issue. If those parties are b7E -3, 4, 5, 6 not able to negotiate a resolution, the prosecutor on the case must be notified to obtain his or her assistance in securing a protective order from the court handling the case. It is recommended that the order include, at a minimum, a direction to each member of the defense team to individually certify, under oath and in writing, that he or she has taken no materials that are considered

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

contraband under federal law away from the government-controlled facility upon completion of the defense examination, and that he or she has not caused any contraband to be sent off site.

(U//~~FOUO~~) If a defense expert represents to the court that it is not feasible to bring his or her tools and equipment to the government facility, the FBI may supply forensic tools and equipment, including appropriate forensic tool licenses, limited to the forensic tools and equipment currently used by the FBI at the time of the request.

**4.3.6.5.2.3. (U) Special Guidelines for Regional Computer Forensic Laboratories in State or Local Cases**

(U//~~FOUO~~) For purposes of handling DE reasonably believed to contain contraband in state and local cases, RCFLs should follow the guidelines listed above whenever possible to prevent the contraband from being redistributed and the victims revictimized. However, with respect to purely state or local cases, RCFLs are obligated to follow state or local court orders governing discovery.

**4.3.6.6. (U)** [REDACTED]

**4.3.6.6.1. (U) Disseminating** [REDACTED]

(U//~~FOUO~~) Case agents may, with the supervisor's approval, provide copies of the [REDACTED] to authorized law enforcement, prosecutors, and [REDACTED] in furtherance of a lawful purpose and consistent with the terms of the search warrant or other legal authority.

b7E -3, 4, 5

(U//~~FOUO~~) All personnel who handle DE must document dissemination of the [REDACTED] in the case notes, case report, and CART database, if applicable. [REDACTED]

(U//~~FOUO~~) Once the DE has been submitted to the ECF, the case agent may copy and disseminate copies of the [REDACTED] and associated reports. If the case agent makes copies of the [REDACTED] he or she is required to label the media in the same manner as the original (e.g., classification markings, banners, file number, and handling caveats).

**4.3.7. (U) Approved Tools**

(U//~~FOUO~~) Approved tools must be used by all DE personnel during the [REDACTED]

b7E 3, 4, 5

(U//~~FOUO~~) Approved tools for processing DE are listed on the [REDACTED] Use of many approved tools requires successful completion of OTD/DFAS-approved training.

b7E -3, 4, 5

(U//~~FOUO~~) In addition to tools listed on the approved tool list, [REDACTED]

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

[REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) For each approved version of each tool, the approved tool list provides information about the forensic processes for which the tool is approved, as well as the known limitations of the tool. DE personnel are responsible for understanding these limitations prior to the use of the tool on DE.

#### 4.3.7.1. (U) Adding Approved Tools

(U//~~FOUO~~) OTD/DFAS must approve tools in accordance with OTD/DFAS test and validation protocol and based upon appropriate scientific and evidentiary criteria.

(U//~~FOUO~~) Recommendations to add tools to the approved tool list may be submitted to the OTD/FSU. Tool testing, validation, and verification must be coordinated through OTD/DFAS/FSU, although actual testing may be performed by personnel from other divisions or agencies, as approved by OTD/DFAS.

#### 4.3.8. (U) [REDACTED]

(U//~~FOUO~~) Case agents should coordinate with OTD [REDACTED]

[REDACTED] Case agents should be aware that the use of unapproved [REDACTED] is discouraged. [REDACTED]

b7E -3, 4, 5, 6

(U//~~FOUO~~) When using [REDACTED]

#### 4.3.9. (U) Requests for [REDACTED]

##### 4.3.9.1. (U) Examinations of Digital Evidence in FBI Cases

b7E -3, 4, 5

(U//~~FOUO~~) Except as authorized in this PG (see Appendix E, "Examination of FBI Evidence by [REDACTED]"), all evidence generated by FBI criminal and [REDACTED] must be submitted for forensic examination or forensic analysis to an FBI laboratory or a forensic program authorized by the FBI Science and Technology Branch (STB). "Forensic examination(s)" or "forensic analysis[es]" is either:

- (U//~~FOUO~~) Generated as part of a process applied by a recognized forensic discipline of the American Society of Crime Laboratory Directors (ASCLD) or the ASCLD-Laboratory Accreditation Board (ASCLD-LAB) or the International Standards Organization (ISO).
- (U//~~FOUO~~) Commonly described or recognized as "forensic" or otherwise relating to the analysis of evidence by scientific or technical means or manner of evidence by or through an expert witness, as defined by the Federal Rules of Evidence (or their applicable equivalent) or as pronounced by rule or ruling of any court or tribunal.

(U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

**4.3.9.2. (U) Transfer of Evidence**

**4.3.9.2.1. (U//~~FOUO~~)** [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) [REDACTED]

(U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5

**4.3.9.3. (U) Chain of Custody**

(U//~~FOUO~~) In criminal investigations, once FBI evidence has been [REDACTED]

b7E -3, 4, 5

[REDACTED] is responsible for maintaining any chain of custody on all original and derivative evidence [REDACTED] created through the examination process until the completion of all trials and appeals. FBI personnel may not retain duplicate evidence or samples of evidence [REDACTED] without the prior written concurrence of the AD, OTD.

**4.3.9.4. (U) Noncircumvention of FBI Policies**

(U) A referral authorized by this PG may not be used, in whole or in part, to purposefully effectuate or passively benefit from activity that would otherwise violate FBI policies, including:

• (U) [REDACTED]

b7E -3, 4, 5

• (U) [REDACTED]

**4.3.9.5. (U) Service Requests in Support of Administrative or Civil Matters**

(U//~~FOUO~~) FBI personnel and facilities [REDACTED] may not accept service requests to provide DE services in administrative or civil matters. The AD, OTD may grant exceptions after consultation with OGC [REDACTED] In considering requests for exceptions, the AD, OTD must determine:

b7E -3, 4, 5, 6

- (U) Whether such support would constitute an acceptable use of appropriated funds.
- (U) The impact on the FBI of using available examiner and equipment resources in support [REDACTED]
- (U) The cost to the FBI in having to provide personnel to testify in a civil matter, as well as being deposed and completing other civil discovery.
- (U) Other relevant factors presented by particular situations.

b7E -3, 4, 5

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

(U//~~FOUO~~) These limitations do not preclude providing DE support for FBI internal investigation matters or for RCFLs to provide DE support [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) If the FBI receives civil or administrative legal process (e.g., a subpoena) in connection with DE services performed for a criminal [REDACTED] the individual served must coordinate with his or her CDC/ADC or OGC counsel for guidance, as applicable.

#### 4.3.10. (U) Reexaminations

##### 4.3.10.1. (U) Definition of Examination

(U//~~FOUO~~) An examination is defined as a forensic process whereby a forensic examiner reviews digital evidence [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) Examination of data previously reviewed by a DExT is not considered a reexamination.

##### 4.3.10.2. (U) Overview of Reexaminations

(U//~~FOUO~~) Unless approved by the AD, OTD, as outlined below, examinations will not be conducted on any evidence that has been previously subjected to the same type of technical examination (hereafter referred to as a "reexamination.")

(U//~~FOUO~~) A reexamination occurs when evidence already subjected to a technical examination [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) This requirement is intended to:

- (U//~~FOUO~~) Eliminate duplication of effort.
- (U//~~FOUO~~) Ensure that the integrity of the evidence is maintained.
- (U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5

o (U//~~FOUO~~) [REDACTED]

o (U//~~FOUO~~) [REDACTED]

o (U//~~FOUO~~) [REDACTED]

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

**4.3.10.3. (U) Requesting a Reexamination**

(U//~~FOUO~~) Within the FBI, reexaminations may only be requested via an EC that has been approved by the head of the requesting field office. ECs must be addressed to the AD, OTD and routed through the UC, FSU and the appropriate CART FO program manager. [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) The request must include a letter from the USAO (or a letter from the district attorney if a state or a local case or a letter from the staff judge advocate [if applicable] in the case of a military investigation), containing:

- (U//~~FOUO~~) The extraordinary circumstances compelling the requested reexamination.
- (U//~~FOUO~~) A detailed explanation of the facts and circumstances surrounding the request.
- (U//~~FOUO~~) All existing service requests.
- (U//~~FOUO~~) All existing legal authorities.
- (U//~~FOUO~~) All prior examination results, notes, and reports pertaining to the previous examinations or reviews, or an explanation as to why this material is not available.

(U//~~FOUO~~) In the event of exigent circumstances [REDACTED]

b7E -3, 4, 5

**4.3.10.4. Approval of Reexamination Requests**

(U//~~FOUO~~) Upon receipt of a request for re-examination, OTD will review the request and supporting materials to determine if a particular examination request is a reexamination for the purpose of seeking the approval of the AD, OTD.

After a determination that the requested examination is or is not a reexamination, a recommendation for the AD of approval or denial will be prepared. OTD will consider the following factors:

- (U//~~FOUO~~) Scope of the requested reexamination
- (U//~~FOUO~~) Responsiveness of the prior examination to previous and current service requests or legal authorities
- (U//~~FOUO~~) Types of tools used in the prior examination or review (e.g., generally accepted forensic tools)
- (U//~~FOUO~~) Location of agency and type of facility that performed the prior examination or review [REDACTED]
- (U//~~FOUO~~) Nature of prior review or examination (including whether prior examination substantially followed or was analogous to FBI CART SOPs)

b7E -3, 4, 5

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

- (U//~~FOUO~~) Whether documentation of prior examination or review provides sufficient detail (including whether there are indicia of a completed examination) [REDACTED] b7E -3, 4, 5

- (U//~~FOUO~~) Background and certification of previous examiner
- (U//~~FOUO~~) Purpose of previous review or examination

(U//~~FOUO~~) The AD, OTD will consider the request for reexamination and, after coordination with OGC [REDACTED] as needed, approve or deny the request. Notice of approval or denial of the reexamination request will be transmitted via EC (to FBI field offices or FBIHQ divisions) [REDACTED] b7E -3, 4, 5, 6. If approved and if required by the circumstances, the approval document may also outline any conditions or limitations placed on the reexamination. The approval documentation must be maintained in the examination file.

(U//~~FOUO~~) Questions regarding whether a service request constitutes a reexamination should be directed to the appropriate DFAS unit.

(U//~~FOUO~~) The case agent must make all necessary notifications to the prosecutor concerning potential [REDACTED] that is or may be created as a result of the reexamination. b7E -3, 4, 5

#### 4.3.11. (U) Advanced Technical Analysis

(U//~~FOUO~~) With respect to DE within their domains of expertise, advanced technical analysis of DE may only be performed by [REDACTED] b7E -3, 4, 5

##### 4.3.11.1. (U) [REDACTED]

(U//~~FOUO~~) Requests for advanced analysis must be made via a service request. All service requests must be submitted via EC or, where available, an automated request through the approved OTD [REDACTED] using an open FBI case file or a request for assistance from [REDACTED] b7E -3, 4, 5, 6 an [REDACTED] to the field office or RCFL.

##### 4.3.11.2. (U//~~FOUO~~//LES) [REDACTED]

(U//~~FOUO~~//LES) [REDACTED]

##### 4.3.11.3. (U) Forensic Audio Video Image Analysis [REDACTED]

(U//~~FOUO~~) All requests for [REDACTED] must be submitted to OTD/FAVIAU via EC or other appropriate documentation identified by FAVIAU. b7E -3, 4, 5, 6

##### 4.3.11.4. (U//~~FOUO~~//LES) [REDACTED]

(U//~~FOUO~~//LES) All requests for [REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

4.3.11.5. ~~(U//FOUO//LES)~~ [REDACTED] b7E -3, 4, 5, 6

~~(U//FOUO//LES)~~ All requests for [REDACTED]

**4.3.12. (U) Assigning Requests to Examiners and Digital Evidence Backlog Definition**

~~(U//FOUO)~~ In order to more accurately assess a backlog of DE requests, the backlog is defined as "any unassigned request that is over 30 days old." To ensure an effective and efficient workflow, supervisors should assign service requests as examiners become available to actively address those requests. At no time should a service request be assigned to avoid being identified as backlog.

~~(U//FOUO)~~ The goal is to more accurately track digital forensic backlog by identifying requests that the field office does not have the resources to address. To further facilitate an accurate accounting of backlog, service requests should be limited to no more than ten unique items. The case agent or requestor should list out the items in the service request and rank them in order of priority to the investigation [REDACTED] b7E -3, 4, 5

~~(U//FOUO)~~ Service requests can be entered directly into the CART database by the case agent or by CART personnel on behalf of the case agent. Service requests entered by CART personnel into the CART database must be inputted within one week of receipt, regardless of other proprietary software/databases used to manage service requests in individual field offices and RCFLs. Offices using the Digital Evidence Management System (DEMS) are exempt from this requirement.

**4.4. (U) Testifying Regarding Digital Evidence Processing**

**4.4.1. (U) Computer Analysis and Response Team Forensic Examiners; Forensic Audio, Video and Image Analysis Unit Examiners; Computer Scientists-Field Office; and Operational Technology Division, Digital Forensics and Analysis Section Technical Experts**

~~(U//FOUO)~~ CART FEs, FAVIAU examiners, CS-FOs, and OTD/DFAS technical expert personnel, based upon their training and experience, are expected and authorized to provide expert opinion testimony within the scope of their duties, in accordance with DOJ and other applicable ethical requirements and as supported by their examinations and the scientific principles underlying their applicable disciplines.

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

**4.4.2. (U) Digital Extraction Technicians and Computer Analysis and Response Team Technicians**

(U//~~FOUO~~) Personnel processing or handling DE as DExTs or CART techs may only provide fact-based testimony consistent with their roles, as they are only trained to the technician level to operate specific categories of tools and conduct specific procedures in accordance with applicable SOPs. These individuals are not expected to possess the requisite breadth and depth of knowledge necessary to provide expert opinion testimony. Instead, DExTs and CART techs may only, if qualified, testify as expert factual witnesses. The scope of their testimony must remain confined to factual assertions concerning the operation of their tools or the application of their procedures (as opposed to, for example, providing opinions on computer forensics or computer operations in general).

**4.5. (U) Seeking Legal Advice**

(U//~~FOUO~~)

b7E -3, 4, 5

UNCLASSIFIED//~~LES~~  
(U) Digital Evidence Policy Guide

## 5. (U) Summary of Legal Authorities

---

- (U) PD 0102D, Operational Technology Division Statement of Authorities and Responsibilities
- (U) 28 CFR § 0.85 (general functions of the FBI): provides that the FBI investigate violations of the law, collect evidence, operate the FBI laboratories, [REDACTED] b7E -3, 4, 5  
[REDACTED] (see specifically, 28 CFR § 0.85(a), (d), (g) and (l)).

~~UNCLASSIFIED//~~LES~~~~  
(U) Digital Evidence Policy Guide

## 6. (U) Recordkeeping Requirements

### 6.1. (U//~~FOUO~~) FBI Central Recordkeeping System

(U//~~FOUO~~) DE must not be uploaded into the FBI's central recordkeeping system or any other FBI administrative or records management system (e.g., FBI Net). The FBI's central recordkeeping system (currently Sentinel) is the FBI's official recordkeeping system for all case file management. Nonrecord materials, per the legal definition of federal records, must not be placed in the recordkeeping system. Nonrecord materials include any copies preserved for convenience or reference. Although the FBI's central recordkeeping system has the ability to accept many documents and file types as either serials or attachments to both ECs and forms, current policies dictate the guidelines for what material is authorized to be placed in the FBI's central recordkeeping system. All original DE (1B) and ELSUR evidence (1D) must be maintained and handled per evidence procedures and guidelines, and as such, original digital and ELSUR evidence must not be serialized, attached to any document, maintained, or stored in the FBI's central recordkeeping system. [REDACTED] b7E -3, 4, 5

[REDACTED] may be retained in the 1A or 1C section of the case file and thus may be serialized into the FBI's central recordkeeping system. Under no exception may contraband material be serialized into the FBI's central recordkeeping system.

[REDACTED]

### 6.2. (U) Additional Information on Recordkeeping and Forms Use

- (U) FOU Intranet site
  - (U) DEL Quality Assurance Intranet site
  - (U) DEL Training Intranet site [restricted access]
  - (U) DIOG
  - (U) [REDACTED] b7E -3, 4, 5
- [REDACTED]

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

### Appendix A: (U) Final Approvals

<b>POLICY TITLE</b> <i>Digital Evidence Policy Guide</i>	
<b>Date of Last Renewal</b>	N/A
<b>Publish Date</b>	2016-07-31
<b>Effective Date</b>	2016-07-31
<b>Review Date</b>	2019-07-31
<b>APPROVALS</b>	
<b>Sponsoring Executive Approval</b>	<b>Brian K. Brooks</b> Deputy Assistant Director Operational Technology Division
<b>General Counsel Approval</b>	<b>James A. Baker</b> General Counsel
<b>Final Approval</b>	<b>Amy S. Hess</b> Executive Assistant Director Science and Technology Branch

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

## Appendix B: (U) Sources of Additional Information

(U) Please review the following Intranet sites for additional information:

(U//~~FOUO~~) All of the below are to be marked (U//~~FOUO~~). [REDACTED] b7E -3, 4, 5, 6

[REDACTED] They are not to be identified to the public.

- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]
- (U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5, 6

OTD OFFICES	OTD PHONE NUMBERS, INTRANET SITES, AND ADDRESSES
OTD Deputy Assistant Director Technical Analysis and Support Branch	
OTD Section Chief Digital Forensics and Analysis Section	
OTD Assistant Section Chief Digital Forensics and Analysis Section, Digital Evidence Lab Director	
Digital Evidence Help Desk Hours: 7:00 a.m.–5:30 p.m. Eastern standard time Monday–Friday	

b7E -1

**UNCLASSIFIED//~~LES~~**  
(U) Digital Evidence Policy Guide

OTD OFFICES	OTD PHONE NUMBERS, INTRANET SITES, AND ADDRESSES
<div data-bbox="289 447 867 491" style="border: 1px solid black; height: 20px; width: 100%;"></div> <div data-bbox="506 499 646 535" style="text-align: center;">Unit Chief</div>	
<div data-bbox="430 674 724 720" style="border: 1px solid black; height: 20px; width: 100%;"></div> <div data-bbox="506 735 646 770" style="text-align: center;">Unit Chief</div>	
<div data-bbox="336 936 824 980" style="border: 1px solid black; height: 20px; width: 100%;"></div> <div data-bbox="506 991 646 1026" style="text-align: center;">Unit Chief</div>	
<div data-bbox="409 1222 758 1268" style="border: 1px solid black; height: 20px; width: 100%;"></div> <div data-bbox="506 1278 646 1314" style="text-align: center;">Unit Chief</div>	
<div data-bbox="341 1509 844 1556" style="border: 1px solid black; height: 20px; width: 100%;"></div> <div data-bbox="506 1568 646 1604" style="text-align: center;">Unit Chief</div>	

b6 -1  
b7C -1  
b7E -1, 4, 6

**UNCLASSIFIED//~~LES~~**  
(U) Digital Evidence Policy Guide

<b>OTD OFFICES</b>	<b>OTD PHONE NUMBERS, INTRANET SITES, AND ADDRESSES</b>
<div data-bbox="279 464 870 510" style="border: 1px solid black; height: 22px; margin-bottom: 10px;"></div> <div data-bbox="505 518 646 554" style="text-align: center;">Unit Chief</div>	
<div data-bbox="418 737 721 785" style="border: 1px solid black; height: 23px; margin-bottom: 10px;"></div> <div data-bbox="505 791 646 829" style="text-align: center;">Unit Chief</div>	

b6 -1  
b7C -1  
b7E -1, 4, 6

UNCLASSIFIED//~~LES~~  
(U) Digital Evidence Policy Guide

**Appendix C: (U) Contact Information**

Operational Technology Division	
Digital Evidence Lab Director	

b6 -1  
b7C -1  
b7E -1, 4, 6

UNCLASSIFIED//~~LES~~  
(U) Digital Evidence Policy Guide

## Appendix D: (U) Definitions and Acronyms

### (U) Defined Concepts

#### (U) Seizure vs. On-scene Imaging vs. Processing

(U//~~FOUO~~) There is often a great deal of digital media at a search site. Because processing and reviewing this media consumes valuable FBI resources, it is important to [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) On-scene, digital media may either be [REDACTED]

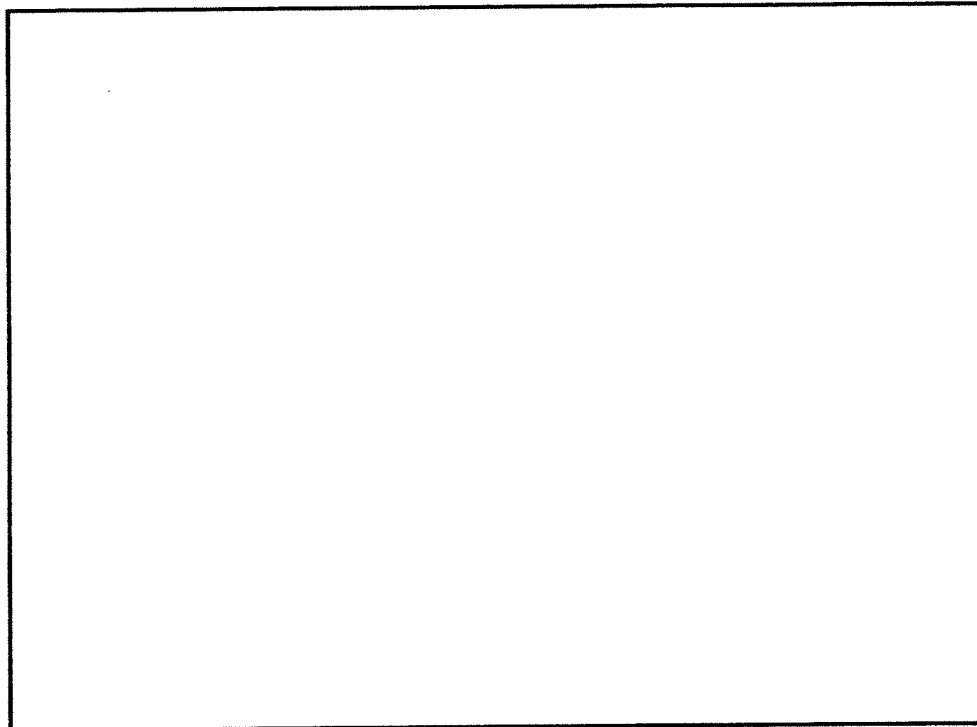
[REDACTED] Otherwise based on legal authority there may be a decision as to whether to [REDACTED]

[REDACTED] It is important to know that imaging is a time-consuming process that may take hours or days, depending upon on the amount of data to be copied.

(U//~~FOUO~~) Once seized DE and images made on-scene are back at an FBI facility, they may be processed using kiosks or preview methods [REDACTED]

b7E -3, 4, 5

[REDACTED] U//~~FOUO~~.



b7E -3, 4, 5

Figure 3. (U//~~FOUO~~) [REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

**(U) Imaging (Copying) DE**

(U//~~FOUO~~) DE is an unusual kind of evidence in that, in most cases, it can be copied many times without degrading the original evidence. Most computer users are familiar with copying files. b7E -3, 4, 5

[REDACTED]

(U//~~FOUO~~) In order to preserve and maintain the original evidence as it was found, b7E -3, 4, 5

[REDACTED]

(U//~~FOUO~~) To prevent cross contamination, b7E -3, 4, 5

[REDACTED]

(U//~~FOUO~~) The above processes related to [REDACTED] are described in the CART SOPs.

**(U) Definitions**

(U//~~FOUO~~) **Approved tools:** tools that have been successfully tested and validated for processing DE or are native applications and utilities necessary for viewing files with proprietary formatting. Approved tools are listed on the OTD Intranet site.

(U//~~FOUO~~) **Computer Analysis Response Team technician:** personnel trained and certified by OTD's Digital Sciences Development and Staffing Unit to forensically copy or image DE.

(U//~~FOUO~~) **Computer Analysis Response Team forensic examiner:** FBIHQ or field personnel, typically assigned full time to DE work, who are trained, equipped, and certified by OTD's Digital Sciences Development and Staffing Unit to copy or image DE, search DE, extract data from DE, and are authorized to provide opinions related to DE in court.

(U//~~FOUO~~) **CART on-the-job trainee:** personnel identified by field office management to participate in training, with a commitment toward becoming certified CART FEs.

(U//~~FOUO~~) **CART forensic examiner trainee:** personnel assigned to work toward CART FE certification 100 percent of their time. Typically, these are trainees hired into ITS-FE positions. These may also be CART OJTs who are near the end of their training and have committed 100 percent of their time to CART FE work.

(U//~~FOUO~~) **Content review report:** factual report of SFE information that details who performed the work, when it was performed, what was reviewed and found, and where it was found.

(U//~~FOUO~~) **Computer scientist-field operations:** The CS-FO works as an integral member of an investigative team, supporting FBI investigations and operations. The CS-FO is responsible for providing advanced technical analysis; exploiting data b7E -3, 4, 5

[REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

(U//~~FOUO~~/LES) DFAS technical experts: DFAS [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) **Digital evidence:** data stored digitally on integrated circuits, microcontrollers, chips, tapes, magnetic media, optical media, or other devices that assist in proving or disproving a matter at issue in a case or investigation.

(U//~~FOUO~~) **Digital evidence extraction technician:** personnel trained to copy or image DE and perform simple SFE processes on copies of DE.

(U//~~FOUO~~) **Digital evidence/media handling:** physical treatment of digital media beginning with the initial identification, seizure, packaging, transport, shipment, storage, and control.

(U//~~FOUO~~) **Digital evidence personnel:** personnel who are authorized upon completion of FBI-approved training in the handling and processing of digital evidence/media (i.e., DExT, CART personnel, and FAVP FA).

(U//~~FOUO~~/LES) **Digital evidence processing:** Processing of DE applies to personnel who are trained and tested to process DE, which includes procedures related to on-scene previewing, imaging, memory capture, performing content reviews, DE searches, extraction, preparing reports, and advanced technical analyses [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) **Examination:** forensic process whereby a forensic examiner reviews digital evidence for [REDACTED]

b7E -3, 4, 5

[REDACTED] Examinations have a specific scope, as defined by the supporting legal authority and the service request pertaining to the evidence submitted for examination. The legal authority and service request may define the scope of the examination [REDACTED]

(U//~~FOUO~~) Examination of data previously reviewed by a DExT is not considered a reexamination.

(U//~~FOUO~~) **Expert opinion:** judgment regarding certain facts or data either acquired by an expert's own investigation, testing, or observations and based on his or her knowledge, skill, experience, training, or education in a certain scientific, technical, or other specialized field.

(U//~~FOUO~~) **Expert testimony:** testimony of a witness qualified as an expert (scientific, technical, or other specialized field) by knowledge, skill, experience, training, or education, in the form of an opinion or otherwise. This testimony is based on sufficient facts or data, is the product of reliable principles and methods, and is grounded upon principles and methods that have been applied reliably to the facts.

(U//~~FOUO~~) **Extraction:** DE that has been [REDACTED] and b7E -3, 4, 5 provided for investigative purposes.

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

(U//~~FOUO~~) **Fact witness:** A fact witness has personal knowledge of events pertaining to a case and can only testify to things he or she has personally observed. A fact witness cannot offer opinions.

(U//~~FOUO~~) **Field Audio Video Personnel forensic analyst:** personnel trained to perform basic forensic functions related to audio and video DE.

(U) [REDACTED] b7E -3, 4, 5

(U//~~FOUO~~) **Master copy:** the required copy of DE that is stored on media to be retained and logged on FD-1004, "Federal Bureau of Investigation Evidence Chain of Custody" form. This is a [REDACTED] of the original DE or a logical copy that contains selected files and artifacts from the original DE, such as relevant files from a business server. It is important that the original legal authority be reviewed before making any copies. If there is a question as to whether a copy of the legal authority documents can be retained and/or forwarded, contact OGC or the local CDC.

(U) **Metadata:** A set of data that describes and gives information about other data.

(U//~~FOUO~~) **Original DE:** DE seized at a search scene or otherwise legally obtained and stored in an ECF.

(U) **Random-Access Memory:** a computer system's memory that contains contents of recent applications and data so that they can be accessed quickly when needed by the computer's processor.

(U//~~FOUO~~) **Reexamination:** A reexamination of DE occurs when data/evidence, already [REDACTED] b7E -3, 4, 5

(U//~~FOUO~~) **Regional Computer Forensics Laboratory associate examiner:** former certified CART FE from an agency participating in the RCFL program who has completed his or her commitment to the RCFL, returns to his or her home agency, and continues a relationship with the RCFL to maintain certification and training.

(U//~~FOUO~~) **Report of examination:** The official report of examination used by CART FEs, Forensic Audio Video Image examiners, and other DE technical experts to report the results of [REDACTED] b7E -3, 4, 5

(U//~~FOUO~~) [REDACTED] less than a full copy of the original DE [REDACTED]  
 [REDACTED]

(U) **Volatile memory:** memory that is not retained when power is lost to a device.

(U//~~FOUO~~) **Working copy:** additional full copies of DE derived from the master copy to allow for review by personnel working for or with the FBI in its investigations [REDACTED] b7E -3, 4, 5  
 [REDACTED]

**Acronyms**

AD	assistant director
----	--------------------

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

ADC	associate division counsel
ADIC	assistant director in charge
AG	Attorney General
AGC	assistant general counsel
ASAC	assistant special agent in charge
ASAC	assistant special agent in charge
ASCLD	American Society of Crime Laboratory Directors
AUSA	assistant United States attorney
CART	Computer Analysis Response Team
CD	compact disc
CDC	chief division counsel
CFR	Code of Federal Regulations
CID	Criminal Investigative Division
CIOS	Counterterrorism Internet Operations Section
CS-FO	computer scientist-field operations
CSO	chief security officer
CSO	chief security officer
CTD	Counterterrorism Division

b7E -3, 4, 5

b7E -3, 4, 5

b7E -3, 4, 5, 6

b7E -3, 4, 5

b7E -3, 4, 5, 6

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

DAG	Deputy Attorney General
DARC	Digital Analysis and Research Center
DE	digital evidence
DEFOU	Digital Evidence Field Operations Unit
DEL	Digital Evidence Laboratory
DEMS	Digital Evidence Management System
DExT	digital extraction technician
DFAS	Digital Forensics and Analysis Section
DIOG	<i>Domestic Investigations and Operations Guide</i>
DOJ	Department of Justice
DTA	domestic technical assistance
DVD	digital video disc
DVR	digital video recorder
EC	electronic communication
ECF	evidence control facility
ECT	evidence control technician
ELSUR	electronic surveillance
FA	forensic analyst
FAU	Forensic Analysis Unit
FAVIAU	Forensic Audio, Video, and Image Analysis Unit
FAVP	Field Audio Video Program
FBI	Federal Bureau of Investigation
FBIInet	FBI Intranet

b7E -3, 4, 5

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

FE	forensic examiner
FET	forensic examiner trainee
FSU	Forensic Support Unit
GB	gigabyte
GC	general counsel
IAU	Investigative Analysis Unit (OTD)
IC	Intelligence Community
IED	improvised explosive device
INI	Innocent Images National Initiative
ISO	International Standards Organization
IT	information technology
ITS	information technology specialist
JTF	joint task force
LA	legal advisor
LD	laboratory director
LEA	law enforcement agency
Legat	legal attaché
LES	Law Enforcement Sensitive
MOU	memorandum of understanding
NDA	nondisclosure agreement

b3 -1  
 b7E -2, 3, 4, 5

b7E -3, 4, 5

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

OGC	Office of the General Counsel	
OJT	on-the-job training	
OTD	Operational Technology Division	
PD	policy directive	
PG	policy guide	
PII	personally identifiable information	
PKI	Public Key Infrastructure	
QA	quality assurance	
QAM	<i>Quality Assurance Manual</i>	
RA	resident agency	
RAM	random-access memory	
RCFL	Regional Computer Forensics Laboratory	
SA	special agent	
SAC	special agent in charge	
SD	Secure Digital [card]	
SFE	search, find, extract	
SIM	sensitive investigative matter	

b7E -3, 4, 5, 6

b7E -3, 4, 5, 6

b3 -1  
b7E -2, 3, 4, 5b3 -1  
b7E -2, 3, 4, 5

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

SSA	supervisory special agent
STB	Science and Technology Branch
STLS	Science and Technology Law Section
tech	technician
TOS	Tactical Operations Section
TURK	Time Utilization and Recordkeeping
U.S.C.	United States Code
U.S.C.	United States Code
UC	unit chief
UCFN	universal case file number
USAO	United States Attorney's Office
USB	Universal Serial Bus
VCAC	violent crimes against children

UNCLASSIFIED//~~LES~~  
(U) Digital Evidence Policy Guide

## Appendix E: (U//~~FOUO~~) Examination of FBI Evidence

b7E -3, 4, 5

(U//~~FOUO~~) As discussed in subsection 4.3.9.1, all evidence generated by FBI criminal and [redacted] investigations (including joint investigations) must be submitted for forensic examination or forensic analysis to a laboratory or an authorized forensic program of the FBI STB, unless an exception to policy is approved in accordance with this appendix.

(U//~~FOUO~~) In rare instances, the unique demands of a particular case may prompt a USAO, a DOJ entity, or another prosecutorial or investigative agency to have FBI evidence processed, examined, or analyzed by [redacted]

b7E -3, 4, 5

(U//~~FOUO~~) This procedure is separate and distinct from reexamination (as defined in subsection 4.2.11.2 above). A reexamination occurs when evidence already subjected to a technical examination is reviewed for the same probative data of its content, source, origin, and manner of creation, alteration, or destruction.

(U//~~FOUO~~) Further, [redacted] FBI personnel must follow the guidance in subsection 4.3.9.2 regarding the transfer of evidence. b7E -3, 4, 5, 6

(U//~~FOUO~~) Subject to the referral prohibitions described below (subsection entitled "Mandatory Prerequisites and Discretionary Referral Factors"), the SC, DFAS, after consultation as desired with an AGC of OGC [redacted] may authorize [redacted] and transfer of FBI evidence to a [redacted] certified forensic examiner or a non-FBI laboratory only under the following conditions:

1. (U//~~FOUO~~) After a determination of the existence of the mandatory prerequisites and due consideration and evaluation of the discretionary referral factors described below.
2. (U//~~FOUO~~) After consultation, as may be deemed appropriate with the appropriate prosecutor and the applicable CDC or OGC supervisor.
3. (U//~~FOUO~~) After compliance with the administrative requirements listed below in the subsection entitled "Administrative Requirements."

(U//~~FOUO~~) [redacted]

b7E -3, 4, 5

(U//~~FOUO~~) Within the FBI, [redacted] may only be requested via an EC approved by the requesting field office's division head. ECs should be addressed to the AD, OTD and be routed through the UC, FSU and the appropriate CART Field Operations program manager. [redacted]

(U//~~FOUO~~) The case agent must ensure that the request EC is serialized to the relevant investigative case file. This EC must include:

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

1. (U) The FBI case ID or UCFN.
2. (U) The FBI field office, telephone number, and fax number.
3. (U) The FBI case agent's name.
4. (U) The applicable case prosecutor's name, if known.
5. (U) A description of the original evidence to be released.
6. (U) The full name, address, and telephone number of [REDACTED]

b7E -3, 4, 5

7. (U) A certification that a supervisory prosecutor and a CDC have concurred in the request, and that the supervisory prosecutor has read and understands the FBI's policy that if [REDACTED]

8. (U) The full name and position title of the case agent's SSA.
9. (U) An acknowledgement from the case agent that he or she understands that it is the case agent's responsibility to make all required notifications to the prosecutor concerning [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) [REDACTED] must include a letter from the USAO, or district attorney if a state or local case, [REDACTED]

[REDACTED]

(U//~~FOUO~~) [REDACTED]

(U//~~FOUO~~) Approving [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) Mandatory Prerequisites and Discretionary [REDACTED]

(U//~~FOUO~~) The SC, DFAS must not authorize an [REDACTED] unless the SC affirmatively determines that either of the following prerequisites is met:

(U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5

[REDACTED] the American Society of Crime Laboratory Directors-Laboratory Accreditation Board (ASCLD-LAB) or the International Standards Organization (ISO), in the recognized forensic discipline or subdiscipline relevant to the examination considered for [REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

[REDACTED] b7E -3, 4, 5

(U//~~FOUO~~) [REDACTED]

[REDACTED]

- (U//~~FOUO~~) [REDACTED] b7E -3, 4, 5

[REDACTED]

- (U//~~FOUO~~) [REDACTED]

(U//~~FOUO~~) [REDACTED]

b7E -3, 4, 5

(U//~~FOUO~~) Assuming that the [REDACTED] prerequisites described in the section above are met, the SC [REDACTED] at his or her discretion, may authorize [REDACTED]

[REDACTED]

- (U//~~FOUO~~) Breadth of experience: the number and complexity of forensic examinations/analyses conducted [REDACTED] b7E -3, 4, 5

- (U//~~FOUO~~) Testimonial experience: the experience [REDACTED]

- (U//~~FOUO~~) Report quality: the quantity and quality of written reports produced by [REDACTED] b7E -3, 4, 5

[REDACTED]

- (U//~~FOUO~~) Equipment acceptance [REDACTED]

- (U//~~FOUO~~) Testing and evaluation documentation: whether there exists sufficient test and validation documentation on the equipment, tools, or materials [REDACTED] b7E -3, 4, 5

[REDACTED]

- (U//~~FOUO~~) Written protocols: [REDACTED]

[REDACTED]  
documentation adequate to facilitate the repeatability of results by an equally qualified examiner.

~~UNCLASSIFIED//~~LES~~~~  
(U) Digital Evidence Policy Guide

- (U//~~FOUO~~) Applied quality assurance system: [REDACTED] b7E -3, 4, 5  
[REDACTED]
  - (U//~~FOUO~~) Annual, impartial, testing-based proficiency examinations.
  - (U//~~FOUO~~) Peer review of examination results and reports.
  - (U//~~FOUO~~) Random and/or regular external compliance audits.
- (U//~~FOUO~~) Legal requirements: [REDACTED] b7E -3, 4, 5  
the examiner is employed or conducting forensic examinations has an affirmative procedure to evaluate, determine, and monitor the ability of the examiner to testify in federal court relative to [REDACTED] (or whether there exists a process for evaluating the existence of exculpatory information, which, as a matter of law, must be affirmatively disclosed, with or without request, [REDACTED]  
[REDACTED]
- (U//~~FOUO~~) Law enforcement authority: whether there is a requirement that examinations are conducted by personnel employed by federal, state, or local law enforcement agencies, as may be required by law or under the direct supervision of a sworn law enforcement officer (e.g., *United States v Shrake*, 515 F.3d U.S. 743 (7th Cir. 2008)) or whether the examination processes are conducted by an examiner who is a federal law enforcement officer or who is working at the direction of a federally sworn officer pursuant to 18 U.S.C. § 3105, if applicable.
- (U//~~FOUO~~) Space restrictions: whether the department, agency, or entity under which the examiner operates has an affirmative process in place requiring that examinations of contraband are conducted in law enforcement-controlled space, as required under the Adam Walsh Child Protection and Safety Act.
- (U//~~FOUO~~) Contraband: whether adequate controls exist to prevent unauthorized access or distribution of contraband pursuant to law (e.g., child pornography at 28 U.S.C. § 2252, et seq., or controlled substances pursuant to 21 U.S.C. § 881, et seq.).
- (U//~~FOUO~~) Criminal history/indices check: [REDACTED] b7E -3, 4, 5  
[REDACTED]
- (U//~~FOUO~~) Security requirements: the maintenance of an appropriate security level clearance relative to the FBI evidence being examined or analyzed in conformity with FBI security policies, as well as the facility and information technology (IT) system in which the evidence will be stored and reviewed that is compliant with FBI security policies and [REDACTED] b7E -3, 4, 5
- (U//~~FOUO~~) Occupational safeguard services: whether appropriate [REDACTED]  
[REDACTED]

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

- (U//~~FOUO~~) Depth/adequacy of examination: whether all necessary examinations, routines, and procedures will be conducted by [REDACTED] b7E -3, 4, 5  
 (federal violations frequently require different elements of proof than do state or local violations of the same or similar nature).

- (U//~~FOUO~~) Preservation of original/best evidence: whether the examination process [REDACTED]  
 [REDACTED] b7E -3, 4, 5
- (U//~~FOUO~~) Cost: [REDACTED]  
 [REDACTED]

**(U//~~FOUO~~) Administrative Requirements**

(U//~~FOUO~~) Prior to initiating a request for [REDACTED] b7E -3, 4, 5

[REDACTED]

- (U//~~FOUO~~) Conduct the examination(s) and testify, as required, at all proceedings associated with the case.
- (U//~~FOUO~~) Conduct all necessary examinations, taking into consideration that violations of federal law often require different elements of proof than the same or similar state or local violations.
- (U//~~FOUO~~) Not destroy or impair the admissibility of the evidentiary material.
- (U//~~FOUO~~) Consult either the FBI Laboratory or OTD DEL, as applicable, on scientific and technical aspects for the examination, if needed.
- (U//~~FOUO~~) Notify either the FBI Laboratory or OTD DEL if an examination will consume the evidentiary material.
- (U//~~FOUO~~) Promptly provide a copy of the examination report to either the FBI Laboratory or OTD DEL after the examination is completed.

(U//~~FOUO~~) The OTD DEL must notify the case agent of any prior knowledge regarding the proposed [REDACTED] concerning the examiner's ability to b7E -3, 4, 5 meet the basic standards of practice of the scientific discipline involved in the examination, or the use of practices that may call into question the ability to use the evidence and examination results or administrative results at any judicial or administrative proceedings. This contact will be documented by the case agent, via EC, in the investigative case file.

**(U//~~FOUO~~) Referral Prohibitions**

(U//~~FOUO~~) Disqualified [REDACTED] b7E -3, 4, 5

(U//~~FOUO~~) [REDACTED]

- (U//~~FOUO~~) [REDACTED]

**UNCLASSIFIED//~~LES~~**  
 (U) Digital Evidence Policy Guide

• (U//~~FOUO~~) [REDACTED]

• (U//~~FOUO~~) The FBI has information that it believes [REDACTED]

b7E -3, 4, 5

• (U//~~FOUO~~) [REDACTED]

**(U//~~FOUO~~) Second Opinion Examinations**

(U//~~FOUO~~) [REDACTED] may not be used, in whole or in part, to seek or obtain second opinions or reexaminations regarding a forensic examination/analysis or variations of an examination/analysis already commenced or completed by an FBI STB laboratory without obtaining reexamination authority as described in subsection 4.3.10 of this PG. If authority is sought for a second opinion or reexamination, the case agent must notify the prosecutor that no testimony should be provided on the same technical subject or area or regarding the initial examination (testimony will be provided for the defense if required by law). The case agent must make all required notifications to the prosecutor concerning [REDACTED] material that is created as a result of the second opinion or reexamination.

b7E -3, 4, 5

**(U//~~FOUO~~) "Curbstone" or Informal Evaluations or Advice**

(U//~~FOUO~~) [REDACTED] may not be used, in whole or in part, to seek or obtain "curbstone," ad hoc, or informal opinions or advice by or from non-FBI scientific or technical personnel to assess the potential value of FBI evidence prior to submitting it to FBI STB laboratories (e.g., FBI personnel may not provide FBI evidence to a non-FBI scientific or technical person to obtain an informal, undocumented or "off the record" opinion on whether it should be submitted to an FBI STB laboratory, or what type of examination should be requested).

b7E -3, 4, 5

**(U//~~FOUO~~) [REDACTED] Investigations Prohibited**

b3 -1

(U//~~FOUO~~) [REDACTED]

b7E -2, 3, 4, 5

• (U//~~FOUO~~) [REDACTED]

• (U//~~FOUO~~) [REDACTED]

b3 -1

b7E -2, 3, 4, 5

• (U//~~FOUO~~) [REDACTED]

• (U//~~FOUO~~) [REDACTED]

~~UNCLASSIFIED//LES~~  
(U) Digital Evidence Policy Guide

- (U//~~FOUO~~) Any national security investigation.

~~(U//FOUO)~~ **Documentation Requirements**

(U//~~FOUO~~) The SC, DFAS must prepare an EC containing the approval or denial of [REDACTED] b7E -3, 4, 5 request and the case agent must ensure that the EC is serialized to the relevant investigative case file. This EC must include the date the request was either approved or denied.

(U//~~FOUO~~) In the case of an approved [REDACTED] a certification by the SC, DFAS that he or she has determined that the proposed [REDACTED]

[REDACTED]

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
SHERMAN DIVISION

BRIAN HUDDLESTON,

Plaintiff,

v.

FEDERAL BUREAU OF  
INVESTIGATION and UNITED  
STATES DEPARTMENT OF JUSTICE,

Defendants.

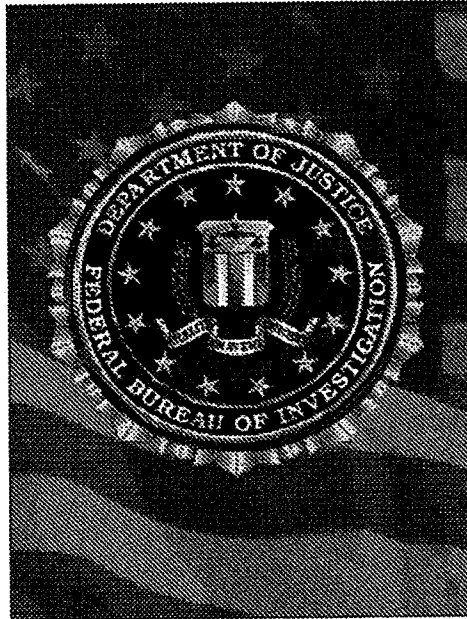
CIVIL ACTION No. 4:20CV00447

**EXHIBIT C**

**UNCLASSIFIED**  
Records Management Policy Guide

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-29-2015 BY J89J28T90 NSICG

## **Records Management Policy Guide**



### **Federal Bureau of Investigation Records Management Division**

**0769PG**

**June 04, 2015**

Revised: 07/01/2015

**UNCLASSIFIED**

**UNCLASSIFIED**  
Records Management Policy Guide

**General Information**

Questions or comments pertaining to this policy guide can be directed to:  
Federal Bureau of Investigation Headquarters (FBIHQ), Records Management Division (RMD)  
Records Policy and Administration Section (RPAS), Policy, Analysis, and Compliance Unit  
(PACU)

**Supersession Information**

See Appendix E of this policy guide for supersession information.

This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit or individual(s) listed above in the general information section of this policy guide.

**UNCLASSIFIED**

## Records Management Policy Guide

**Table of Contents**

<b>1. Introduction.....</b>	<b>1</b>
1.1. Overview .....	1
1.2. Recordkeeping Requirements Policy .....	1
1.3. Purpose of Records Management.....	1
1.4. Benefits of Good Recordkeeping .....	2
1.5. Intended Audience.....	2
<b>2. Roles and Responsibilities .....</b>	<b>3</b>
2.1. Director's Office .....	3
2.1.1. The Director .....	3
2.2. Records Management Division .....	3
2.2.1. Assistant Director.....	3
2.2.2. RMD Front Office.....	3
2.2.3. Records Policy and Administration Section (RPAS).....	4
2.2.4. Records Automation Section .....	4
2.2.5. Record/Information Dissemination Section (RIDS).....	5
2.2.6. National Name Check Program Section (NNCP).....	5
2.3. Office of the General Counsel.....	5
2.3.1. Employment Law Units .....	5
2.3.2. Discovery Coordination and Policy Unit.....	5
2.4. Information and Technology Branch .....	6
2.5. Inspection Division (INSD) .....	6
2.6. Criminal Justice Information Services (CJIS) Division.....	6
2.7. All FBIHQ Divisions/Field Offices/Legal Attaché (Legat) Offices .....	6
2.7.1. Assistant Directors, Special Agents in Charge (SAC), Assistant Directors in Charge (ADIC), Chief Division Counsels (CDC), and other Supervisory Personnel .....	6
2.7.2. Records Liaison .....	6
2.8. All FBI Personnel.....	7
<b>3. Policies.....</b>	<b>9</b>
<b>4. Procedures and Processes.....</b>	<b>10</b>
4.1. Overview .....	10

**UNCLASSIFIED****Records Management Policy Guide**

4.2.	Definition of a Record.....	10
4.2.1.	Questions to Ask in Determining Record Status .....	10
4.3.	Nontransitory Record (Needed for More Than 180 Days) .....	11
4.4.	Transitory Record (Needed For 180 Days or Less) .....	11
4.5.	Nonrecord.....	12
4.6.	Personal Papers .....	12
4.7.	Records Creation and Receipt (Phase 1: Records Life Cycle).....	12
4.7.1.	Records Created by the FBI.....	12
4.7.2.	Supervisory Approval of Administrative Records.....	13
4.7.3.	Records Received from Non-FBI Personnel or Organizations.....	13
4.8.	Records Maintenance and Use (Phase 2: Records Life Cycle).....	13
4.8.1.	Records Requirements .....	13
4.8.2.	Records Systems .....	14
4.8.3.	Central Recordkeeping System–Sentinel.....	14
4.8.4.	Indexing Records .....	14
4.8.5.	Case Management.....	16
4.8.6.	Managing Administrative Records .....	16
4.8.7.	Storing Paper Records.....	17
4.8.8.	Transferring Records .....	18
4.8.9.	Retrieving Records.....	18
4.8.10.	Retrieving Information from Records .....	19
4.8.11.	Electronic Recordkeeping Certification (ERKC) Program.....	20
4.8.12.	Metadata .....	21
4.8.13.	Data Backup Retention.....	21
4.8.14.	Capturing and Preserving Electronic Records .....	22
4.8.15.	Electronic Mail .....	22
4.8.16.	Nontransitory Record E-mails (Needed for More Than 180 Days) .....	23
4.8.17.	Filing Nontransitory Record E-Mails in Sentinel .....	24
4.8.18.	Transitory Record E-Mails (Needed 180 Days or Less).....	24
4.8.19.	Nonrecord E-Mails .....	25
4.8.20.	Web Sites.....	26
4.8.21.	Electronic Information Sharing Technologies .....	26

**UNCLASSIFIED****Records Management Policy Guide**

4.8.22.	Imaged Records and Standards for Scanned Documents.....	26
4.8.23.	Standards for Photographic Records .....	27
4.8.24.	Restrictions on FBI Records .....	27
4.9.	Records Disposition (Phase 3: Records Life Cycle) .....	28
4.9.1.	Modification and Destruction of Records .....	28
4.9.2.	Records Retention Plan.....	28
4.9.3.	Purpose of Record Retention Plan .....	28
4.9.4.	Records Not Included in the Records Retention Plan.....	29
4.9.5.	Applying the Records Retention Plan.....	29
4.9.6.	Preservation of Nontransitory Records with Permanent Retention .....	29
4.9.7.	Disposition of Nontransitory Records with Temporary Retention .....	29
4.9.8.	Disposition of Transitory Records .....	30
4.9.9.	Disposition of Investigative and Intelligence Records .....	30
4.9.10.	Disposition of Records Pertaining to Evidence.....	30
4.9.11.	Disposition of Administrative Records: Classifications 319 and 67Q .....	30
4.9.12.	Disposition of Personnel-Related Records.....	30
4.9.13.	Disposition of Draft Documents .....	31
4.9.14.	Disposition of Personal Files .....	31
4.9.15.	Disposition of Nonrecord Materials .....	31
4.10.	Orphaned Records .....	31
4.11.	Reporting Missing Files and Serials.....	32
4.11.1.	Reporting Missing Files and Serials Subject to Legal Hold .....	32
4.12.	Expungement of FBI Records .....	32
4.12.1.	Court-Ordered Expungements.....	32
4.12.2.	Privacy Act Expungements .....	32
4.13.	Unauthorized Destruction of FBI Records .....	32
4.14.	Damage to FBI Records .....	33
4.15.	RMD Records Disaster Team.....	33
4.16.	Vital Records .....	33
5.	<b>Summary of Legal Authorities .....</b>	<b>34</b>

**UNCLASSIFIED**

**Records Management Policy Guide**

**List of Appendices**

<b>Appendix A: Final Approvals .....</b>	<b>A-1</b>
<b>Appendix B: Sources of Additional Information .....</b>	<b>B-1</b>
<b>Appendix C: Acronyms .....</b>	<b>C-1</b>
<b>Appendix D: Contact Information .....</b>	<b>D-1</b>
<b>Appendix E: Supersessions .....</b>	<b>E-1</b>

**UNCLASSIFIED**  
Records Management Policy Guide

## **1. Introduction**

---

### **1.1. Overview**

All Federal Bureau of Investigation (FBI) personnel create, maintain, and use FBI records. It is therefore critical that FBI personnel understand the policies and procedures governing the FBI's Records Management Program.

### **1.2. Recordkeeping Requirements Policy**

The FBI is required by law (Title 44 United States Code [U.S.C.] Chapter 31) to establish and implement agencywide programs to identify, develop, issue, and periodically review recordkeeping requirements for records of all agency activities at all levels and locations and across all media.

Recordkeeping requirements provide the regulatory means to implement adequate and proper documentation requirements. They provide specific instructions developed by subject matter experts for the collection of information or the maintenance of documents for FBI functions or programs. Recordkeeping requirements can range from broad, governmentwide guidance found in statutes and regulations to office-specific instructions on the preparation of a certain report. Each FBI Headquarters (FBIHQ) division, field office (FO), and legal attaché (Legat) office must, with the assistance of the Records Management Division (RMD), incorporate applicable laws, regulations, or other requirements pertinent to the organization's program responsibilities into recordkeeping requirements for the documentation of its programs.

### **1.3. Purpose of Records Management**

The RMD's mission is to ensure that the right records are created, made available to the right people at the right time and for the right reasons, and disposed of, according to the disposition authorities approved in the FBI Records Retention Plan.

FBI records must be adequate, authentic, legally sufficient, and secure to ensure all FBI legal, fiscal, administrative, and business needs are met. Without complete and accessible records, the FBI cannot conduct investigations, gather and analyze intelligence, assist with the prosecution of criminals, effectively perform its critical missions, or efficiently conduct its day-to-day business.

The FBI is committed to ensuring its Records Management Program:

- Supports law enforcement and national security operations.
- Facilitates documentation of official decisions, policies, activities, and transactions.
- Facilitates timely retrieval and sharing of needed information.
- Ensures business continuity.
- Controls the creation and growth of FBI records.

## **UNCLASSIFIED**

### **Records Management Policy Guide**

- Reduces operating costs by managing records according to the FBI's business needs and by encouraging appropriate disposition practices pursuant to the FBI Records Retention Plan.
- Improves efficiency and productivity through effective records storage and retrieval methods.
- Ensures compliance with applicable laws and regulations.
- Safeguards the FBI's mission-critical information.
- Preserves the FBI's history.
- Implements technology to support records management activities.

#### **1.4. Benefits of Good Recordkeeping**

Adequate and proper recordkeeping ensures that information is available to safeguard the legal and financial rights of the federal government, the FBI, and persons directly affected by the FBI's activities. It ensures the accountability of the FBI to the President of the United States, the United States Congress, the United States courts, and the American people. Additionally, it supports the administration of justice and effective law enforcement and national security operations throughout the FBI's worldwide operations.

Conversely, deficiencies in the management of FBI records impair the FBI's ability to carry out its essential functions and may result in inquiries and investigations by oversight bodies, as well as adverse public perceptions of the FBI's efficiency, accountability, and management. Records mismanagement can also result in adverse judicial rulings during the discovery process.

#### **1.5. Intended Audience**

This policy guide (PG) applies to all FBI personnel. The term "FBI personnel" includes any individual employed by, detailed to, or assigned to the FBI, including members of the armed forces; experts or consultants to the FBI; industrial or commercial contractors, licensees, certificate holders, or grantees of the FBI, including all subcontractors; personal service contractors of the FBI; or any other category or person who acts for, or on behalf of, the FBI, as determined by the FBI Director.

**UNCLASSIFIED**  
Records Management Policy Guide

## **2. Roles and Responsibilities**

---

### **2.1. Director's Office**

#### **2.1.1. The Director**

The Director of the FBI:

- Ensures that records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions are created and preserved.
- Has delegated records management authority to the assistant director (AD) of RMD.

### **2.2. Records Management Division**

#### **2.2.1. Assistant Director**

The AD of RMD will:

- Serve as the FBI records officer, establishing and overseeing a comprehensive FBI-wide Records Management Program.
- Oversee the management of FBI records throughout their life cycles, including records creation, maintenance and use, and disposition of recorded information in all formats.
- Appoint an FBI-wide vital records officer who oversees the FBI's Vital Records Program, in accordance with the *Vital Records Policy Guide (0794PG)*.

#### **2.2.2. RMD Front Office**

##### **2.2.2.1. Training Services Unit (TSU)**

TSU will:

- Provide records management training and guidance to all FBIHQ divisions, FOs, Legats, groups, and organizations throughout the FBI.
- Ensure all FBIHQ divisions, FOs, and Legats are informed of, and trained in, their responsibilities related to the creation, maintenance, and disposition of FBI records.
- Provide guidance and training to FBI personnel on storing and securing records to reduce the risk of damage and loss of information.
- Provide guidance and training to FBI personnel on saving or mitigating the loss of information in records and restoring original records to a useful condition, if possible.

**UNCLASSIFIED**

**Records Management Policy Guide**

**2.2.3. Records Policy and Administration Section (RPAS)**

RPAS will:

- Collaborate with the Records Automation Section (RAS) in the development of records management policies for electronic media.
- Work with the Information and Technology Branch (ITB) and RAS to manage and maintain a policy-compliant records management application (RMA) as part of the FBI's enterprise architecture.
- Establish and disseminate policies and procedures governing the creation, organization, maintenance, use, preservation, disposition, and transfer of all FBI records, regardless of medium or format.
- Conduct periodic FBI records reviews and evaluations to ensure compliance with records management policies and procedures.
- Develop and maintain a network of records liaisons in all FBIHQ divisions, FOs, and Legats, and ensure they receive adequate training to carry out their responsibilities.
- Manage and regularly update the FBI Records Retention Plan and coordinate requests for, and receipt of, all disposition authorities with the National Archives and Records Administration (NARA).
- Manage the storage and maintenance of records.
- Manage the transfer of permanent records to NARA and the destruction of temporary records that have met their retention periods.
- Implement legal holds received from the Office of the General Counsel (OGC).
- Process records modification, permanent charge outs, and expungement requests.
- Conduct and manage FBI-wide record inventories.
- Oversee the storage and maintenance of records in FBIHQ storage areas and advise FBI personnel regarding their records storage and maintenance activities.

**2.2.4. Records Automation Section**

RAS will:

- Collaborate with RPAS in the development of records management policies for electronic media.
- Provide document conversion services (both imaging and optical character recognition) through the Document Conversion Laboratory (DocLab).
- Conduct electronic recordkeeping certification (ERKC) reviews of all information systems used in the conduct of FBI activities.
- Work with the ITB and RPAS to manage and maintain a policy-compliant RMA as part of the FBI's enterprise architecture.

## UNCLASSIFIED

### Records Management Policy Guide

- Plan and assist with the development, management, and maintenance of the enterprise RMA, in coordination with information technology (IT) divisions, offices, and groups.
- Ensure proper records management requirements are incorporated into the design and deployment of new information and knowledge management systems, which include monitoring system compliance with records management requirements.
- Coordinate and guide the incorporation of electronic recordkeeping (ERK) requirements into IT system development.
- Coordinate and guide the incorporation of recordkeeping requirements into the enterprise RMA file plan as records disposition schedules are updated or added.

#### **2.2.5. Record/Information Dissemination Section (RIDS)**

RIDS will:

- Plan, develop, direct, and manage responses to requests for FBI information in accordance with the requirements of the Freedom of Information Act (FOIA) (5 U.S.C. Section [§] 552); the Privacy Act of 1974 (5 U.S.C. § 552a); [FOIA] Executive Order (EO) 13392, *Improving Agency Disclosure of Information*; EO 13526, *Classified National Security Information*; and other applicable Presidential, Attorney General, and FBI policies, procedures, and other mandates, judicial decisions, and Congressional directives.
- Coordinate with OGC's Discovery Coordination and Policy Unit (DCPU) regarding specific FOIA requests.
- Manage the prepublication review program.

#### **2.2.6. National Name Check Program Section (NNCP)**

The NNCP will research, analyze, and disseminate information from FBI records, according to the requirements of the NNCP, in order to respond to requests from customer agencies (EO 10450).

### **2.3. Office of the General Counsel**

#### **2.3.1. Employment Law Units**

The Employment Law Units will assist with the expungement of information from employee personnel records.

#### **2.3.2. Discovery Coordination and Policy Unit**

DCPU will:

- Set the scope, duration, and other characteristics of legal holds.
- Notify FBI personnel of their legal hold obligations.
- Notify FBI personnel of legal hold rescissions.

**UNCLASSIFIED**

Records Management Policy Guide

- Assist FBI personnel with the adjudication and dissemination of record information.

**2.4. Information and Technology Branch**

The ITB will work with RMD, in coordination with the OGC, to plan and deploy a legally compliant RMA as part of the FBI's enterprise architecture.

**2.5. Inspection Division (INSD)**

INSD will:

- Monitor records management compliance in FBI FOs, using records review results provided by RMD's RPAS.
- Coordinate with RPAS's Policy, Analysis, and Compliance Unit (PACU) to conduct focused records reviews, as appropriate.

**2.6. Criminal Justice Information Services (CJIS) Division**

CJIS will send record modifications and expungement requests to the RMD's RPAS.

**2.7. All FBIHQ Divisions/Field Offices/Legal Attaché Offices**

**2.7.1. Assistant Directors, Special Agents in Charge (SAC), Assistant Directors in Charge (ADIC), Chief Division Counsels (CDC), and other Supervisory Personnel**

ADs, SACs, ADICs, CDCs, and other supervisory personnel will:

- Appoint records liaisons to assist RMD in the development and implementation of records management policies and procedures.
- Ensure their respective FBIHQ divisions, FOs, and Legats comply with the RMD's policies by creating, approving, and maintaining adequate and proper documentation of all official programs and activities, including properly indexing in Sentinel or other electronic recordkeeping systems when appropriate.
- Provide resources and time to enable FBIHQ division, FO, and Legat personnel to participate in and complete records management requirements and training.
- Appoint FBIHQ division/FO/Legat vital records officers to work with the FBI-wide vital records officer to identify vital records, in accordance with the Vital Records Policy Guide (0794PG).

**2.7.2. Records Liaison**

The records liaison will:

- Represent an FBIHQ division, an FO, or a Legat by coordinating with RMD on all records management policies, procedures, and programs.
- Understand records management concepts and federal records management laws and regulations.

## UNCLASSIFIED

### Records Management Policy Guide

- Review proposed records management policies within an FBIHQ division, an FO, or a Legat, and provide coordinated review responses to the RMD.
- Oversee the creation and maintenance of records in FBIHQ divisions, FOs, or Legats, and advise FBI personnel in their respective divisions, FOs, and Legats on FBI recordkeeping requirements.
- Monitor records destruction and records transfers to ensure compliance, in coordination with RPAS's Records Disposition Unit (RDU), with any legal holds issued by OGC.
- Provide training on records management policies and procedures, in coordination with RMD's TSU.
- Coordinate with RMD to assist with the resolution of issues involving FBIHQ division, FO, and Legat files.
- Oversee continued inventory of paper records.
- Conduct periodic records audits and inventories, in coordination with RPAS.
- Report promptly to the program manager, Records Protection and Recovery Program, about damage to records.
- Report missing hard-copy case files and serials promptly to RPAS's RDU and for classified material, to the division and/or chief security officer (CSO) via the Security Incident Reporting System (SIRS).
- Report missing hard-copy case files and serials that are subject to legal hold promptly to OGC's DCPU. Report missing classified material to the division and/or CSO via SIRS system owners.

Systems owners will coordinate with RAS to ensure the ERKC process is complete and all documentation is accurate and accessible.

#### **2.8. All FBI Personnel**

All FBI personnel will:

- Create and maintain adequate, complete, accurate, and proper documentation of FBI programs, investigations, activities, decisions, and transactions.
- Ensure the records they create and/or maintain are filed appropriately in an approved central recordkeeping system, such as Sentinel, and are properly indexed when appropriate.
- Ensure all records made or received while in the FBI's service have been properly recorded or properly and legally disposed of prior to separation from FBI service, in accordance with approved retention schedules.
- Cooperate with FBIHQ division, FO, and Legat records liaisons in the creation, maintenance, and disposition of FBI records.

**UNCLASSIFIED**

Records Management Policy Guide

- Ensure all deletion, destruction, or removal of FBI records complies with policies and procedures established by RMD.
- Comply with legal hold obligations and rescissions.

**UNCLASSIFIED**

Records Management Policy Guide

**3. Policies**

---

RMD establishes the requirements, procedures, and policies necessary to ensure FBI personnel manage records effectively to meet the FBI's business needs and to comply with applicable laws and regulations. This PG sets forth those requirements and procedures.

All FBI personnel must comply with the policies and procedures contained in this PG.

**UNCLASSIFIED**  
Records Management Policy Guide

## **4. Procedures and Processes**

---

### **4.1. Overview**

Records management policies and procedures apply to each phase of a record's life cycle:

- Phase 1: Creation and/or receipt (see subsection 4.7.)
- Phase 2: Maintenance and use (see subsection 4.8.)
- Phase 3: Disposition (see subsection 4.9.)

In order to determine what policies and procedures apply to each phase of a record's life cycle, it must first be determined what kind of information is at issue: a record (nontransitory or transitory), a nonrecord, or a personal paper. The Records Management User Manual (RM User Manual) provides detailed information and guidance about specific records management procedures to supplement the policies and procedures outlined in this section.

### **4.2. Definition of a Record**

The Federal Records Act of 1950 (see 44 U.S.C. § 3301), as amended, defines records as:

All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. Records do not include library or museum material made or acquired and preserved solely for reference or exhibition purposes or duplicate copies of records preserved for convenience. Recorded information includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

Specific mediums, platforms, and technologies change over time; however, the determination about what constitutes a record remains the same: it is based on content, not form. Communications using advanced electronic tools and media may be records, depending on their content. This PG applies to all records, regardless of physical form or characteristics.

FBI recordkeeping has evolved from paper-intensive records and information management systems to paperless records and electronic information management systems. Today, the FBI's official recordkeeping system is Sentinel, an electronic information management system. All electronic information management systems within the FBI containing records must comply with the policies and procedures governing the management of FBI records.

#### **4.2.1. Questions to Ask in Determining Record Status**

A document, regardless of medium, is considered a record if it contains information and is:

- Required to be documented by law, regulation, policy, or an established business practice applicable to the FBI.

**UNCLASSIFIED****Records Management Policy Guide**

- Pertinent to an FBI investigation (including assessments) or intelligence-gathering activities.
- Reasonably necessary to protect the rights of the government or of an individual affected by government action.
- Reasonably necessary to document or explain the basis for a significant action or decision involving the exercise of government authority.
- Needed to conduct government business effectively.
- Necessary to document other significant operations or administrative matters. Examples include changes in the FBI's organizational structure, changes in FBI-wide or FBIHQ division policies, accomplishment of an FBI mission responsibility, an expenditure of funds, a disposition of FBI property, and compliance or noncompliance with a legal obligation.

**4.3. Nontransitory Record (Needed for More Than 180 Days)**

A nontransitory record is a record needed for more than 180 days that has one or more of the following characteristics: (1) it provides substantive documentation of the FBI's policies and actions, (2) it contains important and/or valuable evidentiary information, and/or (3) it is required to be maintained by law or regulation. A nontransitory record may have a permanent or temporary retention requirement.

A nontransitory record with a permanent retention period is a record appraised by NARA as having sufficient historical or other value to warrant continued preservation beyond the time the record is needed for an agency's administrative, legal, or fiscal purpose. A permanent, nontransitory record will be transferred to, and preserved as part of, the National Archives of the United States after its usefulness to the FBI has ceased. Examples of permanent, nontransitory records include policy files, exceptional case files, and files pertaining to the FBI's "Ten Most Wanted Fugitives." Exceptional case files document the FBI's investigation of significant individuals, events, organizations, precedent-setting programs, unusual investigative methods, and landmark legal cases involving FBI investigations. Additional information about permanent, nontransitory records is available on RDU's Intranet page.

A nontransitory record with a temporary retention period is a record that NARA has determined to be disposable after a specified period of time or after a specific event has occurred. This period may be for one year, or it could span decades. A temporary, nontransitory record has no continuing value after its usefulness to the FBI has ceased.

**4.4. Transitory Record (Needed For 180 Days or Less)**

A transitory record is a record that has only minimal documentary or evidentiary value and is needed for 180 days or less. Transitory records may include:

- Routine information or publications, working drafts, routine office management documentation, suspense and tickler file notices, and other records that do not serve as the basis for official actions, such as notices of holidays, charitable events, and the like.

**UNCLASSIFIED****Records Management Policy Guide**

- Originating office copies of letters of transmittal that do not add any information already contained in the transmitted material.
- Records documenting routine activities and containing no substantive information, such as routine notifications of meetings, scheduling of work-related trips and visits, and other scheduling-related activities.
- Routine communications, such as reminders of existing policies, work-related guidance, and meeting notices.
- Drafts of, or comments on, proposed policies or actions that are not considered or submitted for consideration by the approving authorities.
- "To-do" lists.

**4.5. Nonrecord**

A nonrecord is any material that does not meet the statutory definition of a record. As set forth in 44 U.S.C. § 3301, examples of nonrecord materials include:

- Library materials made or acquired and preserved solely for reference or exhibition purposes.
- Stocks of publications or unprocessed blank forms.
- Extra copies of documents preserved only for convenience of reference.

Note: Not all copies are nonrecord material. Copies of records may be used for different purposes within the FBI, and they may take on record status. For example, copies of other government agency (OGA) records may be maintained by the FBI as records. A nonrecord copy may also become a transitory record or a nontransitory record if substantive notes or comments are added to the document.

**4.6. Personal Papers**

Personal papers are materials that belong to an individual and are not used to conduct FBI business. They are primarily personal in nature and may be in any format or medium. An example of personal papers includes an employee's copy of his or her Standard Form (SF)-50 ("Notification of Personnel Action"). It is important to note that if a document contains both record and personal information, the document must be treated as a record.

**4.7. Records Creation and Receipt (Phase 1: Records Life Cycle)**

Under the Federal Records Act, every federal agency is required to make and preserve records containing adequate and proper documentation of its organization, functions, policies, procedures, and essential transactions. See 44 U.S.C. Chapters 29, 31, and 33.

**4.7.1. Records Created by the FBI**

Every employee, FBIHQ division, FO, and Legat has the responsibility to adequately document activities, decisions, policies, and transactions conducted to further the FBI's mission and to do so according to FBI policies. Documentary materials created in accordance with this responsibility are records.

## UNCLASSIFIED

## Records Management Policy Guide

Only FBI employees may approve official Bureau records. Policy Directive (PD) 0115D, *Approval Authority for Official Bureau Records*, contains additional information.

**4.7.2. Supervisory Approval of Administrative Records**

FBIHQ divisions, FOs, and Legats are responsible for establishing procedures clearly defining what administrative documents require supervisory approval prior to importing and serializing them to administrative case files. Unless specifically designated, supervisory approval is not required for importing and serializing administrative records. When supervisory approval is required, FBIHQ divisions, FOs, and Legats must establish clearly defined procedures for obtaining required signatures that will not impede the timely serialization of records in the administrative case file.

Supervisors are responsible for making sure staff receives training to ensure documentation requirements are followed. Users are responsible for obtaining supervisory approval of division documents that require such approval and for obtaining this approval prior to importing and serializing them in administrative case files.

The only exemption to this procedure is for documents imported through Sentinel's workflow by those individuals who do not have supervisory functionality. In those instances, when adding administrative documents, the creator can make himself or herself the approver and should do so on those administrative-type documents that the creator's particular office has authorized for self-approval.

**4.7.3. Records Received from Non-FBI Personnel or Organizations**

Documents, databases, and other information received by the FBI that the FBI must or does take action in the course of its routine duties and responsibilities are FBI records, even though non-FBI personnel or other organizations created them. Examples of these types of records include electronic mail (e-mail) or facsimiles (fax).

An exception to the above is non-FBI-generated, evidentiary material seized by the FBI or its law enforcement partners acquired through court order, warrant, federal grand jury or administrative subpoena or voluntarily provided in the course of an investigation of a particular case or intelligence assessment. This material is treated as evidentiary property and is managed under a different set of rules and regulations than those defined in this PG. Note, however, the "Evidence Chain-of-Custody" (FD-1004) form documents the management of evidence, and it is a record. For more information regarding evidence, see the *Field Evidence Management Policy Guide* (0780PG) and the *Domestic Investigations and Operations Guide* (DIOG) (0667DPG).

**4.8. Records Maintenance and Use (Phase 2: Records Life Cycle)**

In this phase of a record's life cycle, authentic, reliable, and trustworthy records are readily available (useable) for business purposes and are protected (maintained) from unauthorized alteration, deletion, or destruction.

**4.8.1. Records Requirements**

Federal regulation Title 36 Code of Federal Regulations (CFR) Chapter XII, Subchapter B, requires agencies to take the following actions in this phase:

## UNCLASSIFIED

### Records Management Policy Guide

- Establish recordkeeping systems for filing records and separating records from nonrecord and personal materials.
- Specify official file locations and storage media for all record types.
- Provide standards, guides, and instructions for easy reference to records.
- Provide reference services to facilitate access to records by authorized users.
- Periodically review and audit recordkeeping systems and practices.

#### **4.8.2. Records Systems**

The FBI utilizes many different databases, electronic information systems, and automated records systems to store case or subject data, and each system has its own unique system documentation and distinct records retention requirements. This PG sets forth recordkeeping policies and provides guidance that applies to the content of each system. Questions regarding individual systems should be directed to the responsible system owner. RAS should be contacted for recordkeeping requirements for system content and documentation, as well as ERKC. Additional information is contained in the ERKC Manual.

#### **4.8.3. Central Recordkeeping System–Sentinel**

The FBI uses a central recordkeeping system to maintain its investigative, intelligence, personnel, applicant, administrative, and general files. Records are maintained in the central recordkeeping system using a file classification system. Investigative and intelligence documents relating to specific cases, as well as significant administrative documents appropriate for distribution to other divisions and offices, are serialized in relevant case files.

In July 2012, Sentinel became the FBI's official central recordkeeping system. It is a next generation information and case-management system. It has moved the FBI from a primarily paper-based recordkeeping system to an electronic records management system. The Sentinel Intranet site contains guidance about document management within Sentinel.

#### **4.8.4. Indexing Records**

Indexing is a fundamental requirement for the management of all types of FBI records, regardless of format, medium, or origin. The FBI must maintain an automated index of subjects, references, victims, and complainants to support FBI investigative and administrative matters. Indexing is mandatory, and FBIHQ divisions, FOs, and Legats must ensure required indexing is accomplished. See DIOG, Section 3 and Appendix J, for additional information.

Within Sentinel, indexing is accomplished by creating an "entity" record. The Indexing User Manual for Sentinel contains guidelines that must be followed for entering and searching Sentinel entity records for persons, organizations, or events that are subjects, references, victims, or complainants. It is designed to promote standardized entry and search formats resulting in effective management of the administrative and investigative information collected by the FBI in the performance of its day-to-day activities. RMD's

**UNCLASSIFIED****Records Management Policy Guide**

PACU will conduct monthly reviews to determine the FBI's compliance with the indexing guidance detailed in the manual referenced above.

**4.8.4.1. Records Series and Filing Locations**

Records are filed according to content and use, regardless of their medium, and are divided into record groups (or series) of files. There are two general types of content: program and administrative.

The majority of the FBI's program or mission-related records are arranged in case files related to a specific file classification. FBI file classifications pertain to federal violations over which the FBI has investigative jurisdiction. File classifications also have been assigned to intelligence, personnel, and administrative matters.

Administrative records facilitate routine organizational or "housekeeping" activities and are created by all FBIHQ divisions, FOs, and Legat offices. Examples of administrative records include time and attendance, travel vouchers, purchase orders, and budget preparation documents. Classifications 319 and 67Q encompass most administrative records; however, some administrative files belong in file classifications such as 242 (Automation) and 261 (Security). For administrative records, file the record copy in the respective division, FO, or Legat subfile designated for the office of origin (OO). See DIOG Appendix J for additional guidance in determining the OO.

With specific approval from RMD's Records Storage and Maintenance Unit, pre-Sentinel Legat classification 319/67Q files may be sent to RMD's Alexandria Records Center (ARC) for storage. RSMU will give special consideration to Legat offices that may experience higher risk for maintaining administrative files. To obtain approval to submit Legat administrative files for storage at the ARC, prepare a lead in Sentinel, addressed to the RSMU, and include an inventory of the files, a total box count, and the desired date of shipment. The Records Management User Manual (RM User Manual) contains additional instructions on this topic.

**4.8.4.2. File Plan**

A file plan is a directory of an office's or a program's records. It outlines the main file headings and subdivision headings for each record series and information system in an office. The plan identifies records in all media, including paper, electronic, and audiovisual, that are physically stored in the office; electronic records, whether on a local or remote computer server or on removable media such as compact discs (CD); records on other nonpaper media, such as digital video discs (DVD), audiotapes, and film; and records stored in other office file storage areas. When records are organized in accordance with a file plan, it is easy to periodically move inactive and noncurrent files out of an office area to other storage locations, freeing up needed office and computer space. Section 3 of the RM User Manual contains detailed guidance about file plans, as well as a sample file plan.

The point when files change from pending to closed or inactive is referred to as a file cutoff. File cutoffs identify and control records in manageable blocks, usually organized by fiscal or calendar year. Some files do not have event-driven cutoffs. These files are

**UNCLASSIFIED****Records Management Policy Guide**

identified and cut off based on their retention. Section 4 of the RM User Manual contains detailed guidance about file cutoffs and their implementation.

**4.8.5. Case Management**

FBI personnel must create and maintain authentic and reliable records, establish files, set leads, supervise investigations, index documents, and retain and share information, as specified in DIOG Section 14 and DIOG Appendix J. Consult Section 5 of the RM User Manual for procedural information and records management guidance for:

- Case files.
- File jackets.
- File types.
- Universal Case File Numbers.
- Serializing.
- Subfiles and subfile designators.
- 1A (FD-340) envelopes.
- Compressed files.
- File consolidation.
- Dual-captioned cases.
- Cover sheets and media labels.
- Records managed by the Executive Secretariat (EXEC SEC).

Procedures for subfiles and subfile designators are set forth in subsection 5.6. of the RM User Manual. ITB and FBI personnel must make sure only dashes, alpha, numeric, and/or blank entries are allowed in the subfile name field of case files.

The use of compressed files is no longer authorized. Compressed files were small paper case files (normally one to ten serials in scope) that were opened in the same file classification and placed together in a single file jacket in order to conserve shelving space. See subsection 5.8. of the RM User Manual for additional information.

**4.8.6. Managing Administrative Records**

Classifications 319 and 67Q are designated for administrative and personnel-related records. A subfile has been opened for each FBIHQ division, FO and Legat for each of the 319 and 67Q categories. However, not all FOs will need to use all the established case file numbers. Administrative records should be filed under the classification 319 categories rather than under an investigative or an intelligence classification.

It is not necessary to import each 319 and 67Q document. If a document needs to go through the Sentinel workflow approval process, it should be imported into the appropriate 319 or 67Q file within Sentinel. If the document does not need to go through the Sentinel workflow approval process (e.g., time and attendance records or a

**UNCLASSIFIED****Records Management Policy Guide**

supervisor's drop files), it does not need to be imported into Sentinel. It may be maintained in a shared drive or a paper folder for the applicable retention period. The disposition of 319 and 67Q matters is discussed in subsection 4.9.11, of this PG.

Performance appraisal reports (PAR) must continue to be maintained in paper format with their original signatures. PARs are maintained by the RMD at the ARC.

Section 6 of the RM User Manual contains additional guidance.

**4.8.7. Storing Paper Records**

FBI paper records are stored in FBIHQ divisions, the ARC, FOs, off-site locations, and Legats around the world. All locations are required by 36 CFR §§ 1223-1238 to meet minimum standards to properly store and protect federal records. Section 8 of the RM User Manual contains detailed guidance regarding records storage.

**4.8.7.1. Files at FBI Headquarters**

The RMD's Records Storage and Maintenance Unit (RSMU) is responsible for overseeing the storage and maintenance of records in FBIHQ storage areas and advising FBI personnel concerning records storage and maintenance activities. The ARC is the main facility for storage and maintenance of (1) FBIHQ closed and pending case files, (2) Legat closed files, (3) closed files from inventoried FOs, (4) security and medical subfile of active personnel, and (5) micrographics, all with a classification of SECRET or lower. FBIHQ paper records with a classification higher than SECRET or containing Sensitive Compartmented Information (SCI) or other matters requiring restricted access are stored at FBIHQ in the Special File Room, J. Edgar Hoover Building

b7

**4.8.7.2. Files at Legat Attaché**

A Legat maintains its pending files. The Security Division's (SecD) Legat Support Program ensures Legats are in compliance with FBI, Department of State, and other national requirements pertaining to secure areas, closed storage of classified information up to the SECRET collateral level, and, where applicable, areas accredited as Sensitive Compartmented Information Facilities (SCIF). Most closed Legat files are stored at the ARC. Subsection 9.3. of the RM User Manual contains detailed procedures for shipping records to the ARC.

**4.8.7.3. Files at a Field Office or a Resident Agency (RA)**

The FO headquarters city maintains the FO's pending files. The relevant RA location may maintain its unclassified and classified materials if it is in compliance with the requirements for classified material storage. Detailed guidance regarding classified material storage can be found in the Safeguarding Classified National Security Information Directive and Policy Guide (0632DPG).

**4.8.7.4. Secure Storage Location Requirements**

SecD is responsible for determining the requirements for all storage locations. The "Open Storage Secure Area Checklist" is a checklist of secure area facility requirements guidelines.

**UNCLASSIFIED****Records Management Policy Guide****4.8.7.5. Environmental Storage Policy**

All records, regardless of format or medium, must be stored in accordance with 36 CFR Part 1234, which sets forth environmental standards and preservation requirements. Section 8 of the RM User Manual contains detailed guidance regarding the minimum requirements for environmental storage of federal records.

**4.8.8. Transferring Records**

Detailed guidance on how to transfer records is included in Section 9 of the RM User Manual.

**4.8.9. Retrieving Records**

FBI employees and authorized personnel may request access to stored, paper files. Case files maintained electronically in the FBI's central recordkeeping system (Sentinel) must not be duplicated in paper and filed. Section 10 of the RM User Manual contains detailed guidance about paper records retrieval.

**4.8.9.1. File-Automated Control System**

The File Automated Control System (FACS) was a library system that was used to track the checking out, and returning of, all FBIHQ paper files (investigative, administrative, and personnel). As of fall 2014, FACS is no longer in use.

Subsection 10.1. of the RM User Manual contains additional information about this system.

**4.8.9.2. File Request Automation Project (FRAP)**

FRAP is an electronic system used to request (1) paper files (investigative, administrative, and personnel), (2) closed FO files sent to the ARC for storage as part of RMD's Field Office Inventory Project, and (3) Legat files stored at the ARC. This system has been constructed using SharePoint and InfoPath and is deployed on FBINet (the FBI [classified] Network). Files may be accessed through the FRAP Intranet site by following the instructions for ordering a file. The file is then checked out and either physically or electronically sent to the requester. When physically sent, a copy of the FRAP request form will be attached to the file for easy identification. The FRAP request form must be kept attached to the file.

The FRAP User Guide contains step-by-step guidance and additional information about this system.

**4.8.9.3. Maintaining Custody of Files**

An individual who checks out a file is responsible for the file until it is returned to the RSMU. In order to maintain security and access control over the information contained within the file, the individual must not give or lend the requested file to other FBI personnel. The file must be returned to RSMU and a new request must be completed.

**4.8.9.4. Returning Files**

All files must be returned to the RSMU within 90 days of receipt unless the requester requires additional time. To retain a file longer than 90 days, the requester must seek an

## UNCLASSIFIED

### Records Management Policy Guide

extension through FRAP. The FRAP request form must be attached to the file when a file ordered through FRAP is returned.

#### **4.8.10. Retrieving Information from Records**

##### **4.8.10.1. Outside the FBI**

##### **4.8.10.1.1. Freedom of Information and Privacy Acts (FOIPA)**

FBI records can be requested through FOIPA. The Policy Directive (PD) 0481D, *Freedom of Information Act and Privacy Act Requests* establishes actions to be taken by FBIHQ divisions, FOs, and Legats when asked by the RMD for assistance in responding to records requests.

##### **4.8.10.1.2. National Name Check Program**

The NNCP disseminates information from FBI files in response to name check requests received from federal agencies and other law enforcement entities, including internal FBI offices; components of the legislative, judicial, and executive branches; and intelligence agencies. The NNCP also conducts name check requests of those persons within arms-reach of the President.

##### **4.8.10.1.3. Mandatory Declassification Review**

Mandatory declassification reviews of FBI material are generally requested by NARA, Presidential libraries, and the public. The *Declassification of Classified National Security Information Directive and Policy Guide* (0623DPG) sets forth the policies and procedures for carrying out the declassification requirements articulated in EO 13526.

##### **4.8.10.1.4. Legal Holds**

FBI personnel have an obligation to ensure all records and nonrecords relevant to a pending litigation or reasonably anticipated matter in litigation (or other proceeding, including criminal investigations, prosecutions, and appeals) and other inquiries, investigations, and inspections are identified and protected from destruction or deletion, even as an exception to standard records disposition practices and schedules, until all legal and official uses are concluded and personnel receive written confirmation from OGC when the identification and protection of such information is no longer necessary. Identifying such records and marking them for retention is referred to as a "freeze" or "legal hold." Whenever legal holds are initiated, all regularly scheduled destruction and/or transfer activities are suspended until OGC has notified FBI personnel that the legal hold has been rescinded. The *Legal Hold Policy* (0619D) contains further information concerning when legal holds may be issued and the roles and responsibilities of FBI personnel and others with regard to a legal hold.

##### **4.8.10.1.5. Assistance to Other Agencies**

If FBI documents and information are to be disseminated to other domestic and foreign agencies for use in investigative and intelligence programs, the documentation and records retention requirements for this type of dissemination are contained in DIOG subsections 12.6. and 12.7.

**UNCLASSIFIED****Records Management Policy Guide****4.8.10.2. Personnel Records****4.8.10.2.1. Electronic Official Personnel Folder (eOPF)**

The FBI's official personnel folders (OPF) are available online for FBI employee access via the eOPF application. Access is only available on a UNet (unclassified network) computer with an FBI Internet Protocol (IP) address.

The eOPF provides electronic, Web-enabled access for all federal agency employees to view and manage employment documents. All employees are able to view their own OPFs through the eOPF application. It also includes security measures that ensure the integrity of the system and employee documents in the system. For more information on accessing an eOPF, see the Human Resources Division's eOPF Information Intranet site.

**4.8.10.2.2. Paper Personnel Records**

Personnel records include the applicant case file; the OPFs of agent personnel retired or separated prior to August 2012 and professional staff personnel separated less than five years prior to January 2012; the security (S) and medical (M) subfiles of active personnel; financial subfile (Sub-F); and PARs. Previously, personnel records included the other government service subfile (Sub-OGS); however, the sub-OGS is no longer maintained as a separate subfiles, it has been incorporated in the eOPF. FBI personnel may submit a formal request for copies of their personnel records. The procedure to do this is set forth in subsection 7.2. of the RM User Manual.

**4.8.11. Electronic Recordkeeping Certification (ERKC) Program**

An electronic information system or a knowledge management (KM) system (collectively, system) contains and provides access to computerized FBI records and other information. A system containing records must comply with the policies and procedures governing the management of FBI records. The RMD AD, as the FBI records officer, has the authority to approve, or withhold approval of, any system in use or under development.

The FBI records officer has delegated the review of systems to RMD's Records Management Application Unit (RMAU). No system may be utilized to conduct FBI business and house FBI records without review by the RMAU and final certification by the FBI records officer.

The goal of the ERKC process is to ensure systems comply with recordkeeping requirements, including the proper creation, maintenance, use, and disposition of FBI records. The ERKC process evaluates system compliance with records management criteria. The process is designed to guide systems owners and developers with assessing and incorporating records management criteria into system requirements specifications and ensuring fulfillment through review of documented test results. The ERKC process consists of identifying systems containing records; helping system owners, project managers, and developers understand ERK criteria; ensuring system requirements specifications satisfy ERK criteria; and validating ERK functionality through review of system test results.

## UNCLASSIFIED

### Records Management Policy Guide

The FBI's ERKC Manual defines the authorities, roles, responsibilities, processes, and documentation requirements that govern the certification of FBI-owned and FBI-sponsored IT systems and serves as a guide for system developers, system owners, project managers, and certification team members concerning the activities required for an FBI-owned or FBI-sponsored system to achieve ERKC.

#### 4.8.12. Metadata

Metadata is defined as data describing information—in particular, its context, content (including author), structure, and its management through time. It is critical that metadata used is detailed and descriptive to effectively manage electronic records throughout their life cycles.

Metadata requirements for recordkeeping purposes are jointly established by both the originating program office and by RMD. With adequate metadata, records are retrieved effectively and purged when no longer needed, without having to be printed for records disposition purposes. Policy for incorporating metadata tags into electronically stored information is located in PD 0249D, Metadata Tagging of Electronically Stored Information in FBI Systems, and the ERKC Manual, Appendix B.

#### 4.8.13. Data Backup Retention

The FBI routinely maintains data backups on computer drives or computer media to protect data from system and server failure or from data corruption. All FBI electronic information systems must be backed up to ensure the authenticity, reliability, and integrity of the information within the systems. A full-data backup of each FBI electronic information system is retained until superseded by the next full-data backup, except for FBINet file/print servers (SECRET enclave). For these, a full-data backup is retained for 90 calendar days. See PD 0076, Data Backup Retention, for additional information on this matter.

Legal holds or other special inquiries are the only exceptions to this data backup retention policy. In these instances, backups must be maintained until OGC rescinds the legal hold or other preservation request.

The approved retention period for data backup is formulated as General Records Schedule (GRS) 20, "Electronic Records," Item 8, as specified by NARA, 44 U.S.C. § 3303a(d). The approved retention period for system backups is formulated as GRS 24, "Information Technology Operations and Management Records," Item 4a, as specified by NARA, 44 U.S.C. § 3303a(d). The backup retention plans for mission specific electronic systems are evaluated as part of the development of records retention guidance for the specific system.

IT systems administrators must maintain data backups in accordance with this PG. OGC is responsible for notifying IT systems administrators when there is a need to retain electronic information beyond the standard retention period for a given electronic information system and for notifying the IT administrators when an exception to the approved retention period has expired.

**UNCLASSIFIED****Records Management Policy Guide****4.8.14. Capturing and Preserving Electronic Records**

All FBI personnel bear responsibility for identifying, capturing, and moving electronic records into a recordkeeping system. To ensure proper preservation, personnel must import electronic communications that are nontransitory records into an ERK system such as Sentinel.

Whenever possible, personnel should import electronic communications in the format in which they were generated, otherwise known as "native format." If an electronic communication cannot be imported in its native format (such as a voice message), it should be preserved in another format (e.g., FD-302 or electronic communication [EC]) in the appropriate recordkeeping system, such as Sentinel.

**4.8.14.1.1. Deletion of Electronic Copies**

Copies of documents are often maintained in electronic form, across all enclaves, either on office shared drives, individual workstations, or portable magnetic or optical media (e.g., flash drives, CDs, diskettes, or tapes). Many of these copies are word processing documents and are kept for convenience of reference or reproduction. If these copies are created solely to produce a convenience copy, once it is verified the record is appropriately filed, they should be deleted, unless subject to a legal hold. It is each employee's responsibility to manage these copies on any FBI information system he or she uses.

**4.8.15. Electronic Mail**

E-mail is a frequent means of communication within the FBI, and the information contained in e-mails must be managed accordingly. FBI personnel are responsible for managing the e-mails they send and receive.

FBI personnel with access to the FBI's e-mail systems must determine the record status of e-mails sent from, or received in, their e-mail account(s). An e-mail may be a nontransitory record (needed for more than 180 days), transitory record (needed for 180 days or less) or nonrecord. When doubt exists about whether or not an e-mail is a nontransitory record e-mail, it should be treated as a nontransitory record e-mail and imported into Sentinel or a successor central recordkeeping system.

E-mails (whether record or nonrecord) that are responsive to legal holds, investigations, FOIPA requests, or special inquiries of any kind must be preserved. PD 0619D, Legal Hold Policy, contains further information.

**4.8.15.1. UNet E-Mail**

Communications received via UNet that contain record material must be uploaded to FBINet to ensure proper records management. UNet e-mails should be copied to FBINet and imported into Sentinel to the relevant FBI case file.

To import these unclassified e-mails into Sentinel, use the "UNet to FBINet File Transfer System" (UNet "Uplift") to transfer the e-mail to FBINet, where it can be filed into Sentinel. See the RM User Manual for further instructions on using Uplift.

**UNCLASSIFIED**

## Records Management Policy Guide

**4.8.16. Nontransitory Record E-mails (Needed for More Than 180 Days)**

A nontransitory record e-mail is a record needed for more than 180 days that provides substantive documentation of the FBI's policies and/or actions, contains important and/or valuable evidentiary information, or is required to be maintained by law or regulation. The principal categories of materials to be preserved are records that:

- Document the formulation and/or execution of policies and decisions and the taking of necessary actions.
- Facilitate action by FBI officials and their successors in office.
- Permit Congress or other duly authorized agencies of the government to conduct a proper scrutiny of the FBI.
- Protect the financial, legal, and other rights of the government and of persons directly affected by the government's actions.

Examples include e-mails that document:

- An investigation or an intelligence analysis. Examples of e-mails that fall into this category include:
  - Exchanges between special agents (SA) or OGA personnel discussing case issues.
  - Electronic surveillance (ELSUR) requests.
  - Requests for assistance from other parties.
  - Surveillance reports.
  - Intraoffice records requests and responses that pertain to an investigation or an analysis.
  - Pertinent intelligence analyses received from another agency.
  - Task force requests for additional funding.
- Significant decisions reached at meetings, conferences, or through e-mail exchanges, such as executive decisions creating or modifying an FBI policy.
- Official agreements with entities outside the FBI.
- Quotes from vendors in response to requests for pricing proposals, which are subsequently used as the basis for contract agreements.
- FBI reorganizations.
- On-duty injuries requiring hospitalization.
- Formal assignments of divisional, FO, and Legat roles and responsibilities.
- End of the fiscal year final reports of expenditures, procurement of goods and services, and annual accountability by all FBI personnel for equipment issued to them.

**UNCLASSIFIED**

## Records Management Policy Guide

**4.8.17. Filing Nontransitory Record E-Mails in Sentinel**

FBI personnel must use the Record Marking Tool (RMT) to import nontransitory record e-mails into the appropriate case file in Sentinel. Subsection 12.1. of the RM User Manual contains additional information about the RMT.

Systems such as Microsoft Outlook, Law Enforcement Online (LEO) mail, and UNet mail are communication systems, not electronic recordkeeping systems. To ensure the retention of nontransitory record e-mails in Sentinel, message creators, recipients, or professional staff personnel must complete the steps necessary to scan and import e-mails into Sentinel or a successor central recordkeeping system. Copies of nontransitory record e-mails must be added to the appropriate case file(s) before the original online e-mail message can be deleted. Attachments, as well as transmission and receipt data about the e-mail, must also be saved as part of the record. Transmission and receipt data include the sender's name, date, subject, recipient(s), and any requested return receipts. See Section 12 of the RM User Manual for instructions.

FBI personnel may not create or send a record (transitory or nontransitory) using nonofficial electronic messaging accounts unless the FBI personnel (1) copy their official electronic messaging accounts in the original creation or transmission of the records, or (2) forward complete copies of the records to their official electronic messaging accounts no later than 20 days after the original creation or transmission of the records.

For nontransitory record e-mails, FBI personnel must also complete the steps necessary to import the e-mail into Sentinel:

If the nontransitory record e-mail does not relate to a specific FBI case, the e-mail message should be filed in the related classification zero (0) file, which serves as a holding file for unsubstantiated allegations. For example, if the e-mail message provides general commentary or guidance on bank robbery matters, but does not contain information related to an actual or specific investigation, the message should be filed in the 91-0 file. If a specific case is later opened or identified, the e-mail message can be transferred from the zero (0) file to the relevant case file.

**4.8.18. Transitory Record E-Mails (Needed for 180 Days or Less)**

Transitory record e-mails are e-mails of short-term interest (180 days or less) and have minimal documentary or evidentiary value to the FBI. As is the case with nonrecord e-mails (discussed below), transitory record e-mails should not be preserved in an FBI recordkeeping system. Absent a legal hold, when no longer needed, these e-mails should be deleted by the creator/receiver. Examples of transitory record e-mails include:

- Routine requests for information or publications, such as e-mails sent to the Office of Public Affairs requesting copies of the "Ten Most Wanted Fugitives" poster and copies of replies.
- Quasi-official notices, such as announcements of upcoming events from the sending office. For example, transit subsidy requirements and forms and annual holiday party guidance are transitory records of the sending office.

**UNCLASSIFIED****Records Management Policy Guide**

- Documentation of routine activities, such as meeting notifications, reminders of midyear performance plan reviews, and unit award nominations sent to a division's or an FO's front office.
- Working drafts of proposed policies or documents.
- Routine requests for supplies and similar office management documentation.
- Suspense files and "to-do" lists.
- Confirmation of training registration, conference attendance, or travel plans.
- Messages sent enterprisewide, such as holiday closing notices or Combined Federal Campaign information. While senders may have an obligation to retain messages for a short time, recipients may delete them when no longer needed.

**4.8.19. Nonrecord E-Mails**

A nonrecord e-mail contains information that does not meet the definition of a federal record. A nonrecord e-mail has no documentary or evidentiary value to the business of the FBI and does not require retention beyond its useful life, as determined by the creator and/or recipient, unless subject to an external request or legal hold, as discussed above. Examples of nonrecord e-mails commonly include e-mails that transmit:

- Copies of records, such as ECs already serialized in Sentinel.
- Copies of FBI publications, such as the DIOG, *The Investigator*, or the *Law Enforcement Bulletin*.
- Informal notes and cover notes that are merely informative in nature and do not include content otherwise warranting preservation as records.
- Copies of PowerPoint training slides from FBI-provided courses.
- Electronic versions of blank forms such as the FD-772, "Report of Foreign Travel."
- Copies of notices received by individuals, such as announcements of upcoming blood drives, seminars, Combined Federal Campaign fundraisers, and similar events.
- FBI personnel anniversary, retirement, and other announcements.
- Discussions between personnel about lunch or other non-work-related activities.
- Other notifications of a personal nature.

FBI personnel with access to the FBI's e-mail systems must determine the record status of e-mails sent from, or received in, their e-mail account(s). Across all enclaves, absent a legal hold, nonrecord e-mails should be deleted from all FBI-managed e-mail systems when no longer needed. Care should be taken by FBI personnel not to commingle record and nonrecord information in e-mails. This ensures nonrecord information is not accidentally transferred or retained in any FBI record repository or system.

**UNCLASSIFIED****Records Management Policy Guide****4.8.20. Intranet Sites**

The Federal Records Act applies to all federal agency records, including Intranet-based records (e.g., records created on SharePoint sites). The E-Government Act of 2002 (Public Law 107-347) places a number of public site requirements on the Office of Management and Budget (OMB), NARA, and agencies in the areas of enterprise architecture, information access and security, and accessibility to persons with disabilities.

FBI personnel who use electronic communication venues to reach agreements or to transmit messages on substantive matters relating to FBI activities, including investigative and intelligence activities, must treat the exchange as a nontransitory record. The nontransitory record must be entered into Sentinel or a successor central recordkeeping system.

Many FBI Intranet pages contain organizational charts, publications, graphic presentations, interactive programs, and links to information repositories. RDU, in conjunction with the Information Technology Infrastructure Division (ITID), has developed a disposition authority, N1-065-04-6, for the administrative records associated with the FBI's public Web site, [www.fbi.gov](http://www.fbi.gov). RMAU, in conjunction with RDU, also assists program offices with developing disposition authorities for records maintained on internal and external FBI sites.

**4.8.21. Electronic Information Sharing Technologies**

The FBI encourages the participation of FBI personnel in both internal FBI-sponsored and external United States government (USG)-sponsored electronic information-sharing technologies (EIST) and the use of EIST.

Information exchanged through EIST may constitute record material, even though the EIST may not be an approved FBI recordkeeping system. All information that meets the definition of a federal record, including data and metadata created or received using EIST, must be entered into an authorized FBI recordkeeping system. Records management procedures for FBI-sponsored EIST must be developed in collaboration with RMD and are subject to RMD's approval. RMD's approval must be obtained before FBI personnel establish, configure, and/or operate EIST. See *Social Media and Other Electronic Information Sharing Technologies Directive and Policy Guide* (0579DPG) for additional information.

**4.8.22. Imaged Records and Standards for Scanned Documents**

Both paper and electronic versions must be managed according to RMD's guidance. See the RM User Manual; PD 0774D, *Records Management Standards for Scanned Documents*; and PD 0671D, *Importing Non-Transitory Records into Sentinel and Preserving Certain Investigative Non-Transitory Records in Original Format*, for additional guidance.

Divisions considering the destruction of paper records after conversion to digital images must have authorization to do so from RMD.

**UNCLASSIFIED****Records Management Policy Guide****4.8.23. Standards for Photographic Records**

Photographic records and negatives may have a permanent retention, and many will be maintained for long retention periods. When practical and possible, FBI electronic photographic records that originated in digital format created by using medium- to high-quality resolution settings appropriate for continued preservation must be produced and retained in a manner appropriate to meet recordkeeping standards and requirements. RMD should be consulted for guidance on the standards for the creation, maintenance, and disposition of digital photographic records.

Digital photographic records and negatives generated by the FBI that are evidentiary or documentary in nature and considered FBI records, such as crime scene photographs, must be filed in the related investigative case file and will assume the retention period established for the file.

The *Field Evidence Management Policy Guide* (0780PG) and the *DIOG* set forth additional guidance regarding the storage and disposition of evidence, as well as the accompanying recordkeeping requirements.

**4.8.24. Restrictions on FBI Records**

Certain types of information must be protected from disclosure. Three examples are discussed briefly below. This is not an all-inclusive list; specific statutes may impose additional burdens on disclosures. For more guidance, see *DIOG* Sections 14 and 18.

**4.8.24.1. Sensitive and Restricted Information**

FBI personnel are required to comply with statutory, regulatory, and FBI policy requirements for the protection of certain sensitive and restricted information. Guidance on the application of national security classifications, caveats, and compartmented access requirements is located on the [SecD Intranet site](#).

**4.8.24.1.1. TOP SECRET (TS) Information /Sensitive Compartmented Information**

TS/SCI must not be serialized into Sentinel. However, a placeholder, documenting the existence and attributes of the TS/SCI material, must be created and serialized into Sentinel. For details on the serialization of TS/SCI material, please see the following document, which is posted on the ["One-Shots" library](#) on the [RMD Intranet site](#).

**4.8.24.2. Federal Grand Jury Material**

Federal Rules of Criminal Procedure 6(e) generally prohibits disclosing "matters occurring before the grand jury." *DIOG* subsection 18.6.5. sets forth policies and guidance regarding the receipt, use, disclosure, and storage of grand jury material.

**4.8.24.3. Federal Tax Information**

FBI personnel must protect information contained in tax returns from disclosure. SecD's FTI program manages policy, training, oversight, and coordination of FBIHQ-level efforts and programs with regard to FTI, in accordance with laws and policies and with direction from the Internal Revenue Service (IRS) and the Department of Justice (DOJ).

**UNCLASSIFIED****Records Management Policy Guide**

DIOG Appendix N sets out guidance on the acquiring, handling, storing, and disposition of FTL.

**4.9. Records Disposition (Phase 3: Records Life Cycle)**

RMD is the sole authority for the disposition of FBI records, regardless of location or medium. "Disposition" is a comprehensive term referring to either the permanent transfer of nontransitory records to NARA or the destruction of all other records.

**4.9.1. Modification and Destruction of Records**

RMD is the sole entity with authority to destroy or delete FBI records and is the sole entity that can authorize the destruction or deletion of FBI records. RMD (or its designee) will modify or destroy records, as authorized or required by law and in accordance with approved retention schedules. RMD is also the sole entity with authority to modify or destroy electronic references or pointers in nonrecord automated systems (i.e., Automated Case Support [ACS]), which serve to point the user to the FBI's electronic records systems.

All FBIHQ divisions, FOs and Legats must advise RMD of the need to modify or destroy records. In Sentinel, this can be accomplished by setting a lead to DK-RPAS (RMD Records Policy and Administration Section) and requesting a permanent charge-out (PCO) of the relevant material

**4.9.2. Records Retention Plan**

RDU implements and updates the FBI Records Retention Plan, which governs the retention, disposition, and transfer of all FBI records, regardless of location or format. The FBI Records Retention Plan refers collectively to the GRS as well as the individual disposition schedules (SF-115 "Request for Records Disposition Authority") the FBI submits to NARA for approval.

Disposition schedules are broken down by records series (i.e., file classification) or by system name. For each records series or system, the disposition schedule includes a brief description of the records, a breakdown of the types of records covered by the records series or system, and disposition instructions for each.

**4.9.3. Purpose of Record Retention Plan**

The FBI Records Retention Plan:

- Ensures compliance with the law. Federal agencies are required to have retention schedules for their records, regardless of format.
- Reduces the risk that records will be disposed of before they have met their authorized retention periods.
- Ensures records are retained as long as needed for business purposes and disposed of when no longer needed.
- Facilitates discovery during litigation.
- Protects the FBI from litigation resulting from the destruction of unscheduled records.

**UNCLASSIFIED****Records Management Policy Guide**

- Frees up costly office and computer space, removing records no longer needed for current business activities.

**4.9.4. Records Not Included in the Records Retention Plan**

Records that are not included in the FBI Records Retention Plan or the GRSs are not authorized for disposition. These records must be retained; they cannot be deleted or destroyed. Owners and creators of these records should contact RDU for assistance with hard copy paper records and RMAU for assistance with electronic records.

**4.9.4.1. Creating a New Series of Records**

FBI personnel must contact RDU (paper records) or RMAU (electronic records) if the program, FBIHQ division, FO, or Legat begins creating a new series of records, obtains authorization for a new file classification, creates a new electronic information system, or substantially changes the ways in which records are created and used. RDU and RMAU will work with FBI personnel to analyze retention requirements and develop a retention schedule.

**4.9.5. Applying the Records Retention Plan**

The FBI Records Retention Plan sets forth specific instructions about the length of time records must be maintained. Section 13 of the RM User Manual contains detailed guidance regarding the disposition of records. The RM User Manual supplements the general policy discussion below and should be consulted as a reference tool. Note: Legal holds supersede any destruction guidance provided in the RM User Manual until such holds have been lifted.

**4.9.6. Preservation of Nontransitory Records with Permanent Retention**

The FBI Records Retention Plan designates a small percentage of all FBI records for permanent retention and allows for the destruction of the remainder. "Permanent retention" means a file will never be deleted or destroyed. The file will be processed by RDU and transferred to NARA for continuing retention after a specified number of years following the closing of the case. When an electronic case file is transferred to NARA, it will be deleted from the FBI's electronic system by RDU. NARA will make the file available for researchers studying the FBI's investigations and activities, when appropriate. See Section 13 of the RM User Manual for additional guidance.

**4.9.7. Disposition of Nontransitory Records with Temporary Retention**

Temporary records are records deemed by NARA to have no continuing value after their usefulness to the agency has ceased. These records are not transferred to NARA for preservation, but rather are destroyed either after a fixed period or after a specific event has occurred. Their retention periods may range from months to years. Temporary records are disposed of in accordance with a NARA-approved records schedule, unless those records are subject to a legal hold. RMD is the sole entity with authority to destroy or delete FBI records and the sole entity that can authorize the destruction or deletion of the FBI's temporary records.

## UNCLASSIFIED

### Records Management Policy Guide

#### **4.9.8. Disposition of Transitory Records**

Transitory records do not need to be scanned or imported into Sentinel. They may be deleted by the user/receiver when no longer needed or deleted according to an automated deletion process, unless those records are subject to a legal hold.

#### **4.9.9. Disposition of Investigative and Intelligence Records**

RDU (paper records) and RMAU (electronic records) directly manage the disposition of all investigative and intelligence-related records. This ensures that the complex disposition requirements for these records are accurately and consistently applied. Because most of the mission-related activities of the FBI are documented in investigative and intelligence classifications, offices must retain these case files until RDU or RMAU issues specific disposition instructions or directs the transfer of records to FBIHQ for processing. Offices must not initiate disposition actions without prior guidance from RDU or RMAU.

#### **4.9.10. Disposition of Records Pertaining to Evidence**

Once a case is closed and all investigative needs have been exhausted, non-FBI-generated evidence is returned to the owner/contributor, destroyed, or forfeited. FBI-generated evidentiary and nonevidentiary items, regardless of size, that are documentary in nature and considered FBI records, such as chain of custody forms, agents' notes, crime scene photographs, and laboratory analyses, should be filed in the related investigative case file and will assume the retention period established for the file, unless modified by a legal hold.

The *Field Evidence Management Policy Guide* (0780PG) sets forth the policy regarding the storage and disposition of evidence, as well as the accompanying recordkeeping requirements.

#### **4.9.11. Disposition of Administrative Records: Classifications 319 and 67Q**

All classification 319 and 67Q records must be maintained in Sentinel or in a successor central recordkeeping system.

Most of the FBI's administrative records are temporary records and may be destroyed after their retention periods have expired. This means after a certain period has lapsed, the records can be destroyed with the approval or at the direction of RDU (paper records) or RMAU (electronic records), unless these records are subject to a legal hold. Once the retention period has expired, and authorization has been obtained, eligible classification 319 and 67Q paper serials can be destroyed.

#### **4.9.12. Disposition of Personnel-Related Records**

Personnel subfiles are maintained at the ARC, regardless of the location of the FBI personnel. The disposition of subfiles Sub-M, Sub-S, and Sub-F, is determined by the "Memorandum of Understanding Among the U.S. Office of Personnel Management, the Federal Bureau of Investigation, and the National Archives and Records Administration and Addendums 1, 2, and 3" and the FBI Records Retention Plan.

**UNCLASSIFIED****Records Management Policy Guide**

RDU applies disposition to unsuccessful applicant records in accordance with retention schedules, unless they are subject to a legal hold.

**4.9.13. Disposition of Draft Documents**

Working files, such as preliminary drafts, notes, and other similar materials, are to be destroyed when the final documents have been approved by the FBI official with authority to do so, unless they:

- Are subject to a legal hold.
- Relate to pending FOIPA requests.
- Contain unique information, such as substantive annotations or comments that add to a proper understanding of the FBI's formulation and execution of basic policies, decisions, actions, or responsibilities and were circulated or made available for approval, comment, action, recommendation, follow-up, or to communicate FBI business.
- Have some other business reason requiring retention for reference purposes.

This guidance applies to all drafts created in any medium.

**4.9.14. Disposition of Personal Files**

Personal papers are not federal records and are not imported, serialized, indexed, or filed in FBI records management systems. They should be maintained separately from office records and may be disposed of at the owner's discretion, unless subject to a legal hold or FOIA.

**4.9.15. Disposition of Nonrecord Materials**

Nonrecord material does not need an authorized disposition. It is destroyed when FBI personnel or the responsible office no longer needs it or when the information has served its intended purpose, unless subject to a legal hold or FOIA. As a matter of good recordkeeping practice, FBI personnel should file nonrecord materials separately from records. FBI personnel should review nonrecord materials annually, and materials that are no longer useful should be destroyed.

**4.10. Orphaned Records**

Orphaned records are records left behind by the creators or owners. Orphaned records are sometimes abandoned in offices after personnel have moved or a reorganization has occurred. FBI personnel should be aware of their responsibilities in ensuring records in their custody are not inadvertently left behind during office moves. Similarly, supervisors should ensure that departing FBI personnel manage records in their possession prior to departure. Anyone finding orphaned records should contact the RMD Help Desk, and RMD will help determine the disposition of those records. See subsection 13.13. of the RM User Manual for additional guidance.

**UNCLASSIFIED****Records Management Policy Guide****4.11. Reporting Missing Files and Serials**

Files or serials missing for 30 calendar days or longer must be reported by the records liaison, via EC, to the RDU within 30 calendar days of discovery. Reasonable efforts to locate missing files or serials must be undertaken, and the status of those efforts must be reported to the RDU every 60 days after the initial report is filed. RDU shall report any missing files or serials to NARA that have not been located within six months of the date of the reported loss.

**4.11.1. Reporting Missing Files and Serials Subject to Legal Hold**

If missing files or serials contain documents subject to a legal hold, OGC's DCPU must be notified immediately.

If missing files or serials contain classified material, this must be reported immediately to the division and/or CSO, who will then report it to the Security Compliance Unit at FBIHQ, as directed by PD 0610D, Security Incident Program.

If missing files or serials can be recreated from other sources, the file should be recreated, and the new file must reference that fact. In addition, if a missing file or a serial is recreated from other sources, and the materials are subject to a legal hold, the FBIHQ division or FO must notify DCPU immediately.

The records liaison must contact RDU if, after reporting a missing file or serial, the material is subsequently located.

**4.12. Expungement of FBI Records****4.12.1. Court-Ordered Expungements**

RMD's RPAS is responsible for processing court-ordered requests for the expungement of FBI case files. RPAS does this in accordance with PD 0169D, Expungement of FBI Records.

RPAS only processes expungement requests received directly from the CJIS Division or from OGC. Should an FBIHQ division or an FO receive an expungement request from a local, state, or federal court, the expungement request must be forwarded to the CJIS Division's Criminal History and Investigative Service Unit for processing.

**4.12.2. Privacy Act Expungements**

The Privacy Act allows individuals to request expungement of their records. For example, an individual may ask that erroneous information contained in his or her FBI records be expunged. All Privacy Act expungement requests are referred to the RMD's Record/Information Dissemination Section for processing.

**4.13. Unauthorized Destruction of FBI Records**

All FBI personnel are responsible for preventing the unauthorized destruction, damage, or alienation (removal from FBI custody) of records. The unlawful removal, defacing, alteration, or destruction of federal records may result in penalties, including fines and imprisonment. If files or serials are missing or destroyed due to negligent or willful

## UNCLASSIFIED

### Records Management Policy Guide

misconduct of FBI personnel, the Office of Professional Responsibility (OPR), OGC, and RDU must be notified immediately.

RDU must then report the unauthorized destruction of any files or serials to NARA.

#### **4.14. Damage to FBI Records**

FBI records can be damaged by natural or manmade events or causes. The extent of damage can vary from minimal to extensive and can occur at any time; therefore, all FBI personnel should understand and be able to implement basic salvage operations to reduce continued deterioration of FBI records.

Information about protecting and recovering records is available on RMD's Records Protection and Recovery Intranet site.

Damaged FBI records must be reported to RMD through an EC (FD-1057), using case file 3190-HQ-A1487624-XX, Records Management Matters (replace XX with the FO's two-letter designator). The incident that damaged the documents and the remediation provided must be described in the EC.

#### **4.15. RMD Records Disaster Team**

The RMD Records Disaster Team is a collaborative effort of trained RMD employees who can deploy to any FBI division for predisaster and postdisaster records assistance. Additional information about the Records Disaster Team can be found on RMD's Records Protection and Recovery Intranet site.

#### **4.16. Vital Records**

Vital records are records that are essential to the functions of the FBI's operation during and following an emergency. The loss of these records during a disaster can create gaps in vital information, resulting in the disruption of essential services, exposure to unplanned expenses of financial settlements or loss of revenue, increased vulnerability to litigation, and loss of productivity.

Vital records may be maintained on a variety of media including paper, magnetic tape or disc, photographic film, removable hardware, and microfilm. The Vital Records Program (VRP), as defined in 36 CFR § 1236.14, provides resources to identify, use, and protect the essential operating records needed to meet federal responsibilities under national security or disaster emergencies. The Vital Records Policy Guide (0794PG) contains information about the FBI's Vital Records Program.

**UNCLASSIFIED**  
Records Management Policy Guide

## **5. Summary of Legal Authorities**

---

Several agencies, including NARA, OMB, and the General Services Administration (GSA) share oversight of records management in the federal government. Listed below are citations to the codes, regulations, and authorities most relevant to records management:

- Records Management by the Archivist of the United States and by the Administrator of General Services (44 U.S.C. Chapter 29)
- Records Management by Federal Agencies (44 U.S.C. Chapter 31)
- Disposal of Records (44 U.S.C. Chapter 33)
- Coordination of Federal Information Policy (44 U.S.C. Chapter 35)
- Public Money, Property, or Records (18 U.S.C. § 641)
- Criminal Penalties for Unauthorized Disposal of Federal Records (18 U.S.C. § 2071)
- The Freedom of Information Act (5 U.S.C. § 552)
- The Privacy Act of 1974 (5 U.S.C. § 552a)
- Federal Records (36 CFR Chapter 12, Subchapter B)
- Personnel Records (5 CFR Part 293)
- OMB Circular A-130: *Management of Federal Information Resources*
- U.S. Office of Personnel Management (OPM) Manual, *The Guide to Personnel Recordkeeping* (November 2006)
- Department of Justice Order No. 0801 (March 12, 2014) (establishes policy governing the DOJ Records and Information Management (RIM) Program for the creation, capture or receipt, maintenance and use, and disposition of all DOJ records”

**UNCLASSIFIED**

## Records Management Policy Guide

**Appendix A: Final Approvals**

<b>POLICY TITLE:</b> <i>Records Management Policy Guide</i>	
<b>Primary Strategic Objective</b>	P-1 Streamline administrative and operational processes
<b>Publish Date</b>	2015-06-04
<b>Effective Date</b>	2015-06-04
<b>Review Date</b>	2018-06-04
<b>EXEMPTIONS</b>	
None	
<b>REFERENCES</b>	
See Section 4 and Appendices B and C of this PG.	
<b>APPROVALS</b>	
<b>Sponsoring Executive Approval</b>	<b>Michelle A. Jupina</b> Assistant Director Records Management Division
<b>Final Approval</b>	<b>Kevin L. Perkins</b> Associate Deputy Director

**UNCLASSIFIED**

**Records Management Policy Guide**

**Appendix B: Sources of Additional Information**

- Declassification of Classified National Security Information Policy Guide (0623DPG)
- Domestic Investigations and Operations Guide (DIOG) (0667DPG)
- Social Media and Other Electronic Information Sharing Technologies Directive and Policy Guide (0579DPG)
- FBI Electronic Recordkeeping Certification Manual
- Field Evidence Management Policy Guide (0780PG)
- FRAP User Guide for Non-NNCP Users
- FRAP Intranet site
- PD 0418D, Freedom of Information Act and Privacy Act Requests
- PD 0619D, Legal Hold Policy
- "Managing Your Federal Records: A Guide for FBI Executives"
- PD 0249, Metadata Tagging of Electronically Stored Information in FBI Systems
- Open storage secure area checklist
- Prepublication Review Policy Guide (0792PG)
- PD 0423D, Preservation and Disclosure of Electronic Communications in Federal Criminal Cases
- Records Management Division Intranet site
- Records Management User Manual (RM User Manual)
- RMD Help Desk
- PD 0610D, Security Incident Program
- Sentinel Intranet site
- Indexing User Manual for Sentinel
- PD 0774D, Records Management Standards for Scanned Documents
- PD 0671D, Importing Non-Transitory Records into Sentinel and Preserving Certain Investigative Non-Transitory Records in Original Format
- Vital Records Policy Guide (0794PG)
- "Memorandum of Understanding Among the U.S. Office of Personnel Management, the Federal Bureau of Investigation, and the National Archives and Records Administration" and Addendums 1, 2, and 3
- PD 0457D, RMD Statement of Authorities and Responsibilities

B-1

**UNCLASSIFIED**

**UNCLASSIFIED**

## Records Management Policy Guide

**Appendix C: Acronyms**

ACS	Automated Case Support [system]
AD	assistant director
ADIC	assistant director in charge
ARC	Alexandria Records Center
CD	compact disc
CDC	chief division counsel
CFR	Code of Federal Regulations
CJIS	Criminal Justice Information Services Division
DCPU	Discovery Coordination and Policy Unit
DIOG	<i>Domestic Investigations and Operations Guide</i>
DK-RPAS	RMD Records Policy and Administration Section
DocLab	Document Conversion Laboratory
DOJ	Department of Justice
DVD	digital video discs
EC	electronic communication
EIST	electronic information sharing technologies
ELSUR	electronic surveillance
e-mail	electronic mail
EO	executive order
eOPF	electronic official personnel file
ERK	electronic recordkeeping
ERKC	electronic recordkeeping certification

**UNCLASSIFIED**

## Records Management Policy Guide

Exec Sec	Executive Secretariat
FACS	file automated control system
fax	facsimile
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
FBINet	Federal Bureau of Investigation Network
FO	field office
FOIA	Freedom of Information Act
FOIPA	Freedom of Information and Privacy Acts
FRAP	file request automation report
FTI	federal tax information
GRS	General Records Schedule
GSA	General Services Administration
INSD	Inspection Division
IP	Internet Protocol
IT	information technology
ITB	Information and Technology Branch
ITID	Information Technology Infrastructure Division
JEH	J. Edgar Hoover [Building]
KM	knowledge management
Legat	legal attaché
LEO	Law Enforcement Online

**UNCLASSIFIED**

## Records Management Policy Guide

MAOP	<i>Manual of Administrative Operations and Procedures</i>
NARA	National Archives and Records Administration
NNCP	National Name Check Program
OGA	other government agency
OGC	Office of the General Counsel
OGS	other government service
OMB	Office of Management and Budget
OO	office of origin
OPF	official personnel files
OPM	Office of Personnel Management
OPR	Office of Professional Responsibility
PACU	Policy, Analysis, and Compliance Unit
PAR	performance appraisal reports
PCO	permanent charge-out
PD	policy directive
PG	policy guide
RA	resident agency
RAS	Records Automation Section
RDU	Records Disposition Unit
RIDS	Record/Information Dissemination Section
RM	Records Manual
RMA	records management application

**UNCLASSIFIED**

## Records Management Policy Guide

RMAU	Records Management Application Unit
RMD	Records Management Division
RMT	Record Marking Tool
RPAS	Records Policy and Administration Section
RSMU	Records Storage and Maintenance Unit
SA	special agent
SAC	special agent in charge
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SecD	Security Division
SF	Standard Form
SIRS	Security Incident Reporting System
TS	TOP SECRET
TSU	Training Services Unit
U.S.C.	United States Code
UNet	unclassified network
USG	United States government
VRP	Vital Records Program

**UNCLASSIFIED**

Records Management Policy Guide

**Appendix D: Contact Information**

Records Management Division	
RMD Help Desk phone	<input type="text"/>
RMD Help Desk e-mail	<input type="text"/>

b7.

**UNCLASSIFIED**

Records Management Policy Guide

**Appendix E: Supersessions**

---

This PG supersedes:

- *Records Management Manual* (POL05-0001-RMD)
- PD 0106D, *Reporting Missing Files and Serials*
- PD 0108D, *Disposition Authority for FBI Records*
- PD 0291D, *Supervisory Approval of Administrative Records*
- PD 0332D, *Use of Special Characters and Symbols as Subfile Designators*
- PD 0372D, *Non-record E-mail Retention*
- PD 0131D, *Modification and Destruction of Records*
- 66F-HQ-A1358157-POLI serial 2
- 319W-HQ-A1487698 serial 12
- 319W-HQ-A1487698 serial 325
- 319O-HQ-1487624 serial 545
- *Manual of Administrative Operations and Procedures* (MAOP) Part 1 Section 20-4.1. through 20-4.2.
- MAOP Part 2 Section 2-3.5.
- MAOP Part 2 Section 2-3.11.
- MAOP Part 2 Section 2-4.1. through 2-4.3.8.
- MAOP Part 2 Section 2-4.5. through 2-4.5.29.
- MAOP Part 2 Section 2-5.1. through 2-5.3.1.
- MAOP Part 2 Section 11-5.1.
- MAOP Part 2 Section 11-7.3.